시스코 SD Access Lab v1

마지막 업데이트: 2017년 10월 25일

본 데모에 대하여

미리 구성되어 있는 본 데모는 아래 내용을 포함합니다.

준비사항

아래 항목은 데모를 진행하는데 필요한 구성요소입니다.

테이블 1. 준비사항

필수	옵션
●개인용 컴퓨터	● 시스코 AnyConnect®

솔루션 소개

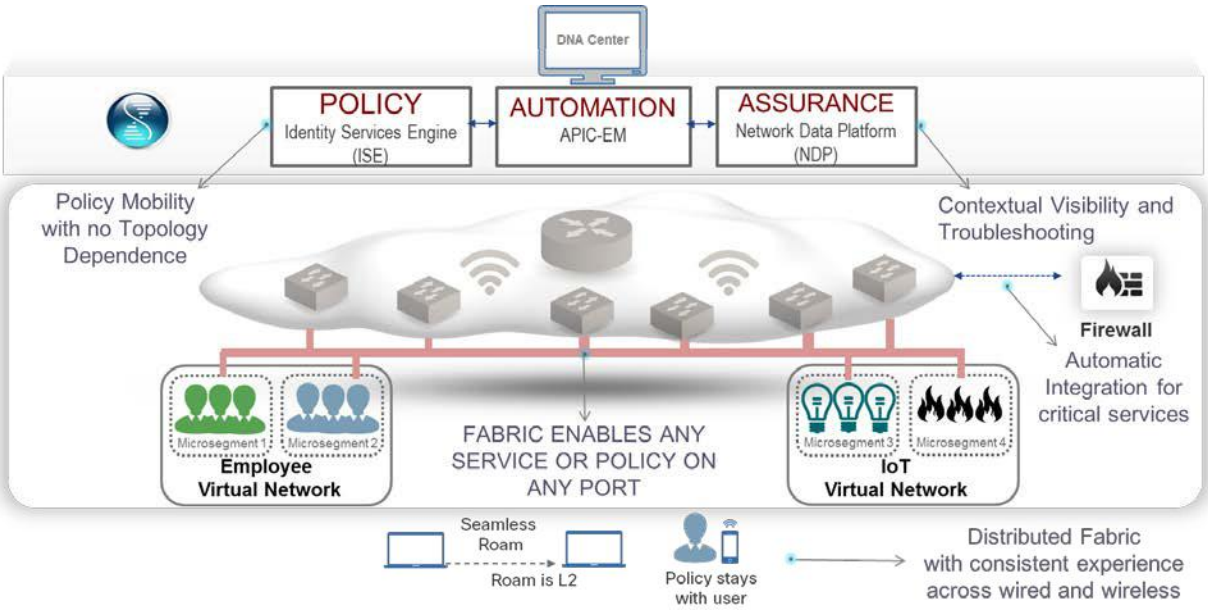
디지털화는 모든 기업들로 하여금 비지니스에 IT 기술을 접목시키도록 환경을 변화시키고 있습니다 . 시스코의 디지털 네트워크 아키텍처 (Digital Network Architecture, DNA)는 아래 내용을 제공하기 위한 목적으로 일련의 설계 원칙을 통해 만들어진 개방형 소프트웨어 기반 아키텍처입니다.

- 보다 빠른 비즈니스 혁신을 위한 통찰력 및 행동
- Automaton 및 Assurance 로 IT 비용 및 복잡성을 줄이면서 비즈니스 및 사용자 기대를 충족
- 조직이 지속적으로 확장하고 성장함에 따라 관련 리스크를 줄이기 위한 보안 및 규정 준수

.

혁신적인 시스코의 소프트웨어 정의 액세스(SD-Access) 솔루션은 네트워크 Edge 에서 클라우드 영역까지 정책 기반의 자동화 기술을 제공합니다. 네트워크 패브릭을 통해 사용자, 엔드 단말 및 IoT 장치에 대한 보안 세그먼테이션 구성이 가능하므로 운영이 대폭 간소화되고 확장성이 있으며 완벽한 가시성을 통해 새로운 서비스를 신속히 제공 할 수 있습니다. SD-Access 는 네트워크 구성(Configuration), 프로비저닝(provisioning) 및 트러블 슈팅과 같은 일상적인 작업들을 자동화함으로써 네트워크 작업에 소요되는 시간을 줄이고 문제해결 능력은 향상 시키며 보안 침해에 대한 영향은 줄입니다. 이로 인해 비즈니스에 대한 CapEx 및 OpEx 비용을 크게 절감할 수 있습니다.

SD-Access 가 가져다 주는 효과



SD-Access 기능

SD-Access 는 새롭게 선보인 DNA Center 애플리케이션을 통해 네트워크 자동화 프로비저닝을 위한 Fabric 기반의 인프라와 탁월한 GUI 환경을 이용하여 통합 보안, 세그먼테이션 및 탄력성있는 서비스 롤아웃을 제공할 수 있도록 설계된 시스코의 차세대 엔터프라이즈 네트워킹 액세스 솔루션입니다.

SD-Access 는 초기 개발단계에서 다음과 같은 주요 기능을 제공합니다 (본 데모에서는 모든 기능을 사용할 수 없습니다):

테이블 2. SD-Access 기능

기능	세부
네트워크 디자인	DNA Center - 디자인 (Design) 앱 ● 네트워크 계층 ● 사이트 프로파일(Profiles) 및 전달(Inheritance) ● 네트워크 설정 ● DNA Center -ISE 통합 ● IP 주소 관리 ● 무선 사이트 디자인 및 SSID 관리 ● 무선 Map
네트워크 프로비저닝 (Underlay)	수동 구성 ● DNA Center 디스커버리, 인벤토리 및 토폴로지 앱 자동 구성 ● DNA Center Design 앱– 프로파일 변환
패브릭 프로비저닝 (Overlay)	DNA Center - 앱 프로비저닝 ● 사이트에 디바이스 할당 ● ISE 내에서 자동 NAD 전달 ● 패브릭 도메인 생성 및 삭제 ● 패브릭 도메인에 디바이스 추가 ○ 콘트롤 플레인(Control Plane) 설정 ○ 경계(Border) 설정 ○ 컨트롤 플레인 및 경계(Border) 콜로케이션 구성 ● SD-무선 ● L2 LISP (ex: Bonjour support)
어드레스 Pool 및 호스트 온보딩	DNA Center - 앱 프로비저닝 ● IP Pool 할당 (유선 또는 무선) ● 동적 인증(Authentication) ● 802.1X, MAB, EasyConnect ● 고급 dot1x 설정 ● 정적 Pool 할당 ● 데이터 및 음성 Pool 할당 ● 멀티캐스트 Pool 할당 (View 전용) (주의: EFT CD3 에서는 멀티캐스트 미지원)
정책 관리	DNA Center - 정책 앱 ● 기존 정책이 학습 됨 ● 가상 네트워크 생성 및 삭제 ● 양방향 (Bi-directional) 정책 ● 패브릭-to-Non 패브릭 정책 지원 (Fabric-to-non fabric) ● 정책 대시보드 ● 응용 프로그램을위한 사용자 정의 확장 가능 그룹 ● 정책 지원 DNA Center - ISE 와 연동한 정책 앱 ● ISE 에서 그룹 생성 및 가져 오기 ● DNA Center 에서의 그룹 정책 정의 ● L4 정책에 대한 사용자 정의 계약(Contract) 생성

SD-Access Lab 진행방식

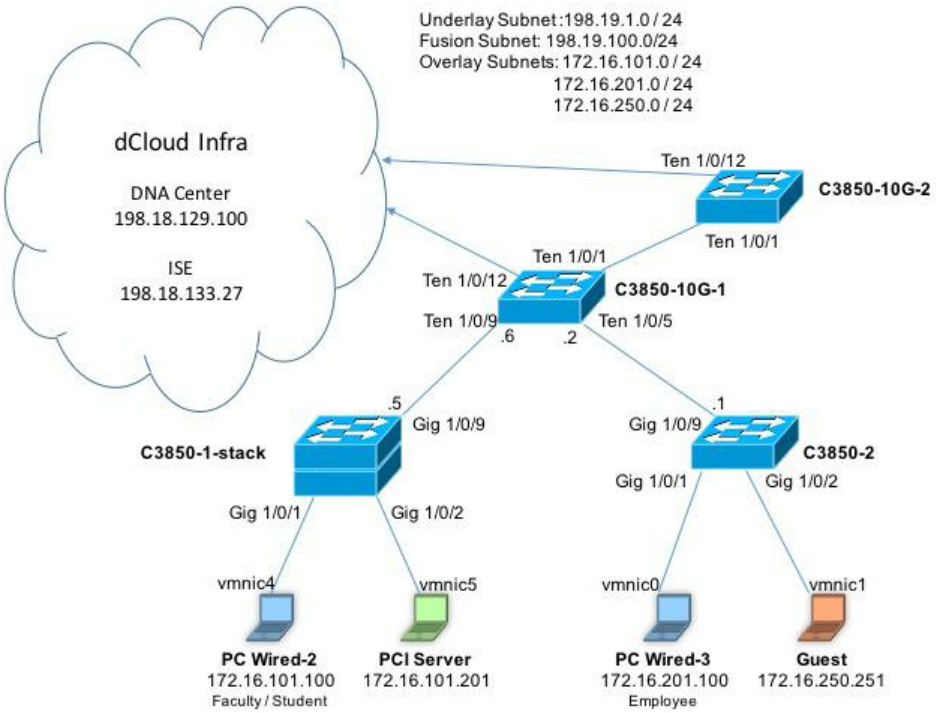
본 dCloud 랩 가이드는 스위치들의 Underlay 환경이 미리 구성되어 있고 DNA Center 와 ISE v2.3 이 사전 설치 및 연동되어 있는 것을 전제로 진행됩니다. 시나리오 환경은 대학교 캠퍼스 구축(University campus deployment)을 예로 들어 설명합니다:

- Lab 은 SD-Access App 과 Tool 을 살펴보고 DNA Center 에 익숙해지기 위한 내용부터 시작합니다.
- DNA Center 를 통해 Underlay 장비를 탐색하고 해당 장치들이 Discover 및 Inventory Tool 을 사용하고 있는지 확인할 수 있습니다. DNA Center 는 토폴로지 Tool 을 통해 해당 장비들을 표시합니다.
- 다음은 Design app 을 이용하여 사이트를 생성하고 해당 사이트를 구성하기 위해 사용하는 공통 속성, 리소스 및 자격 증명 등의 여러 정보들은 DNA Center 관련 작업을 위해 지속적으로 재사용됩니다.
- 그리고 Policy App 과 DNA Center 및 ISE 통합에 대해 간략히 설명합니다.
- Policy App 에서 가상 네트워크(VN)가 생성되며 이를 통해 네트워크 레벨의 세그멘테이션이 구성됩니다. 이 단계에서는 ISE 를 통해 학습된 그룹들이 가상 네트워크(VN)와 연동되고 이 작업을 통해 마이크로 레벨의 세그멘테이션이 구현됩니다.
- 다음으로 중앙 집중식 보안 정책 구성을 위해 정책 관리 프로세스를 이용하며 정책은 ISE 를 통해 확인할 수 있습니다.
- DNA Center 로 돌아가고 탐색된 장비들이 사이트로 프로비저닝됩니다.
- 다음으로는 Overlay 패브릭이 프로비저닝됩니다.
- 검증의 마지막 부분에서는 외부 퓨전 라우터(external fusion router)를 이용해 intra-overlay 및 inter-overlay 라우팅을 구성하고 검증합니다.

구성도

본 데모는 시나리오의 원활한 진행 및 솔루션이 제공하는 각 기능들의 동작 확인을 위해 사전 설정된 구성요소들을 포함하고 있습니다. 대부분의 구성요소들은 별도 제공되는 관리자 계정을 통해 설정이 가능하며 **토폴로지** 메뉴에 있는 구성요소 아이콘을 클릭하면 해당 구성요소에 접근하기 위한 IP 어드레스 및 계정 정보를 확인할 수 있습니다

그림 **1.** 물리 구성도



테이블 3. 장비 세부 정보

IP 주소	구성요소	계정	암호
https://198.18.129.100	DNA Center	admin	C1sco12345
https://198.18.133.27	ISE	admin	C1sco12345
198.18.134.109	C3850-10g-1 (dCloud)	cisco	cisco
198.18.134.110	C3850-10g-2 (dCloud)	cisco	cisco
198.19.1.2	C3850-10g-1 (Underlay)	cisco	cisco
198.19.1.5	C3850-1-stack	cisco	cisco
198.19.1.1	C3850-2	cisco	cisco
172.16.101.100	PC-Wired-2	admin	C1sco12345
172.16.201.100	PC-Wired-3	admin	C1sco12345
172.16.101.201	PCI-Server	admin	C1sco12345
https://198.18.129.100	DNA Center	admin	C1sco12345
https://198.18.133.27	ISE	admin	C1sco12345

dCloud 시작하기

시작하기에 앞서

고객 및 파트너를 대상으로 데모시연을 할 경우 원활한 진행을 위해 본 자료를 가지고 사전에 충분한 연습을 하시기를 권장합니다.

데모 완료 후 새로이 구성을 해야 하는 경우는 세션을 새로 예약하십시오.

사전에 충분한 연습은 성공적 진행을 위한 필수 조건입니다.

세션 예약 및 데모 환경을 준비하기 위하여 아래 절차를 따라 주십시오.

1 dCloud 세션 시작. [가이드]

노트: 세션 예약 후 시나리오의 랩이 활성화 되기까지 최대 45 분 소요됩니다.

2 보다 빠른 환경으로 시나리오 진행을 원하는 경우는 **시스코 AnyConnect VPN 클라이언트** [가이드] 및 **이용자 컴퓨터에 있는 로컬 RDP 클라이언트를 이용해 접속하십시오.** [가이드]

- Workstation 1: **198.18.133.36**, Username: **win7wkst/admin**, Password: **C1sco12345**

노트: dCloud 의 리모트 데스크탑 클라이언트[가이드]를 이용한 접속도 가능합니다. dCloud 가 제공하는 리모트 데스크탑 클라이언트는 데모 세션을 유지시키기 위한 시스템 워크로드를 최소한으로 발생시키기 때문에 리모트 접속에 최적화된 환경을 제공합니다.

3 . Cisco Anyconnect VPN 을 사용하여 연결하지 않으면 dCloud 구성도 스크린에서 Windows 7 및 원격 데스크톱을 선택하십시오. 수동으로 로그인하고자 하는 경우는 자격 증명을 메모해 두십시오.

시나리오 1. Welcome to the DNA Center

스텝:

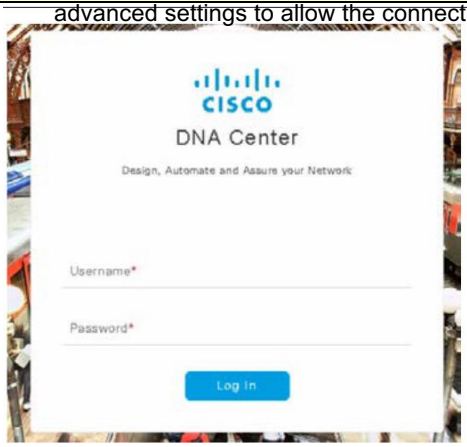
1. 데스크톱에서 Google 크롬 열기.
2. 아래의 로그인 정보를 사용하여 DNA Center 에 로그인하십시오

   사용자 ID: **admin**

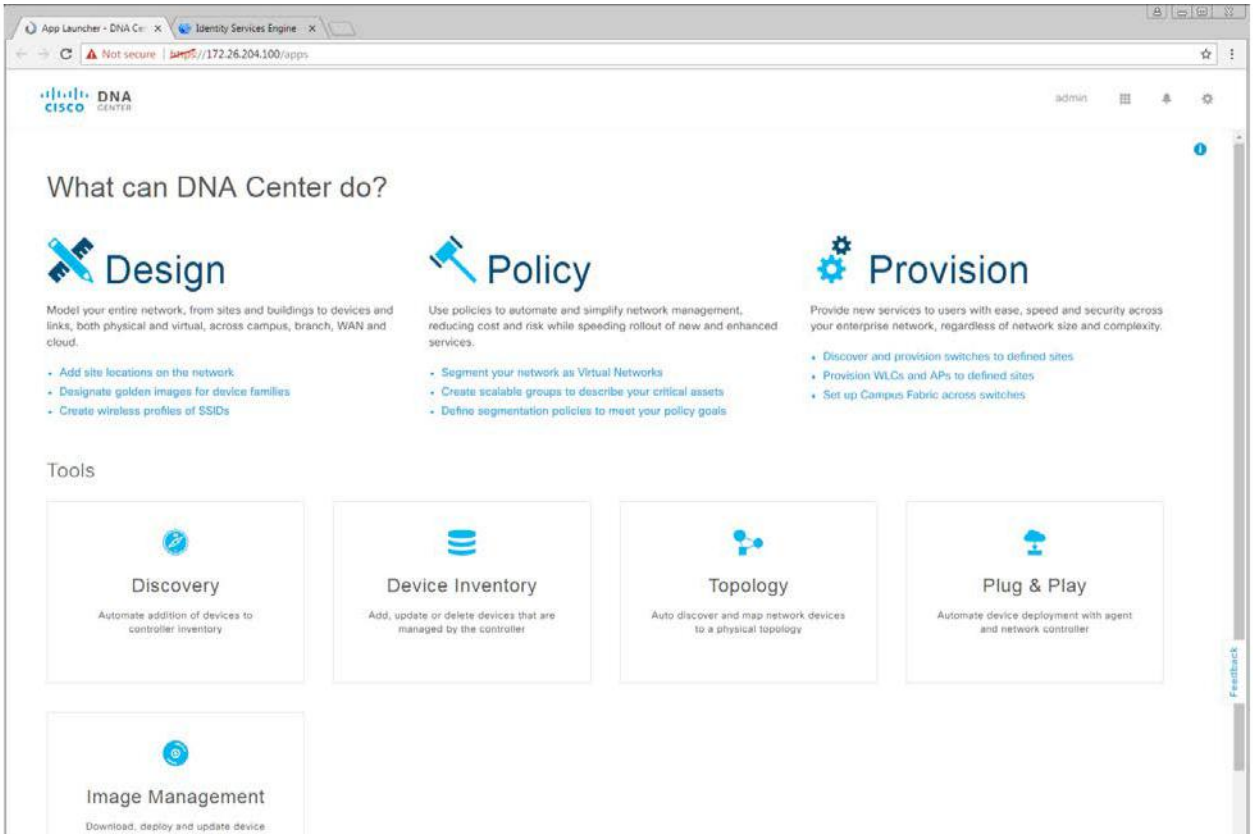
   암호 : **C1sco12345**

노트: DNA Center 의 SSL 인증서를 클라이언트 브라우저가 자동으로 수락하지 않을 수 있습니다. 이 경우 고급 설정을 사용하여 연결을 허용하십시오.

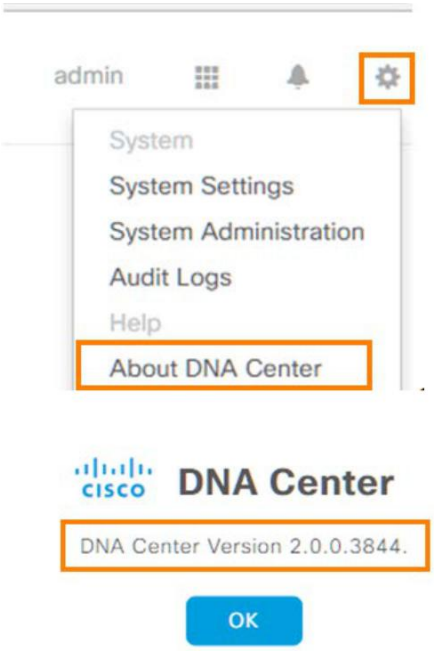
advanced settings to allow the connection.



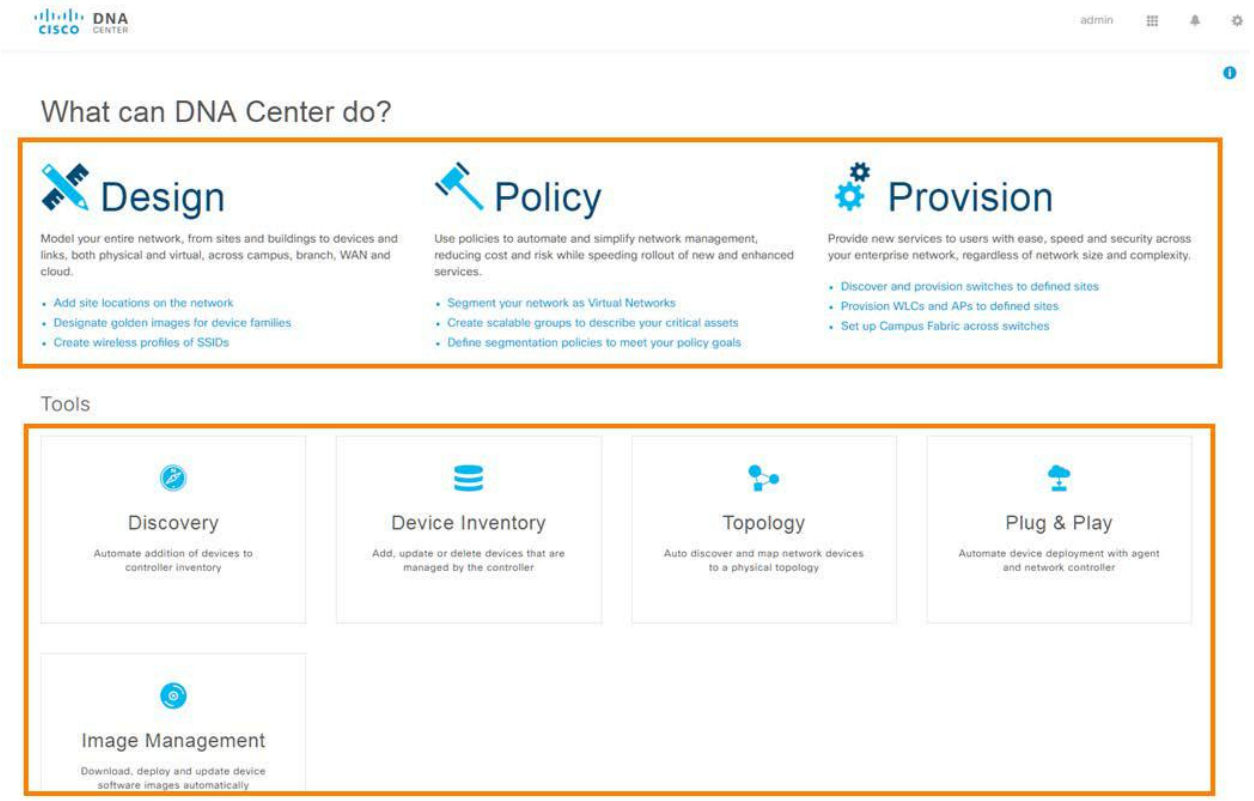
3. 로그인하면 DNA Center 대시 보드 화면이 나타납니다.



4. DNA Center 버전을 보려면 오른쪽 상단의 기어를 (Gear) ⚙ 클릭하고 **About DNA Center** 를 선택하십시오.

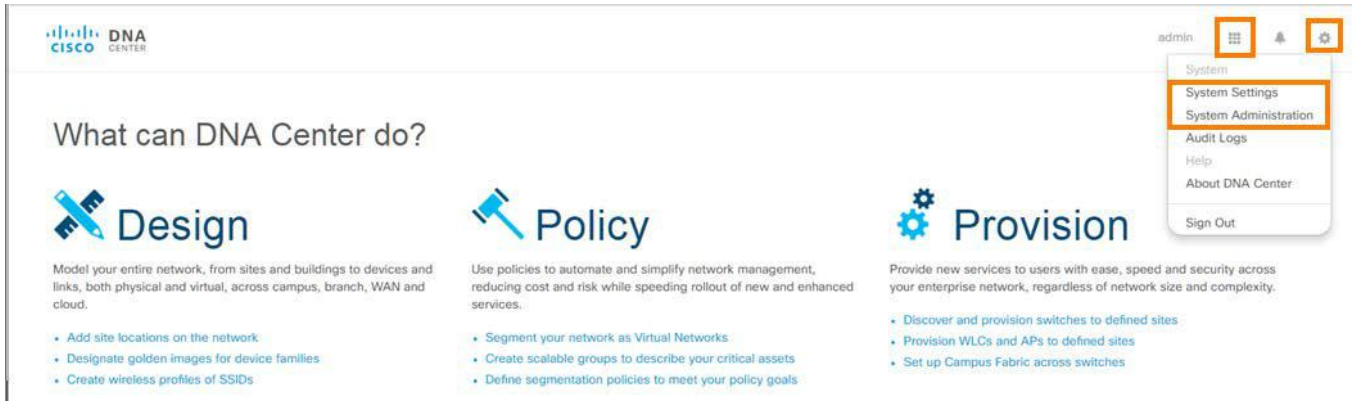


5. DNA Center 의 메인 화면은 **응용(Applications) 프로그램**과 **도구(Tools)** 두 가지 영역으로 구분됩니다. 이 영역에는 SD-Access 환경을 만들고 관리하기위한 응용 프로그램을 포함하고 있습니다.

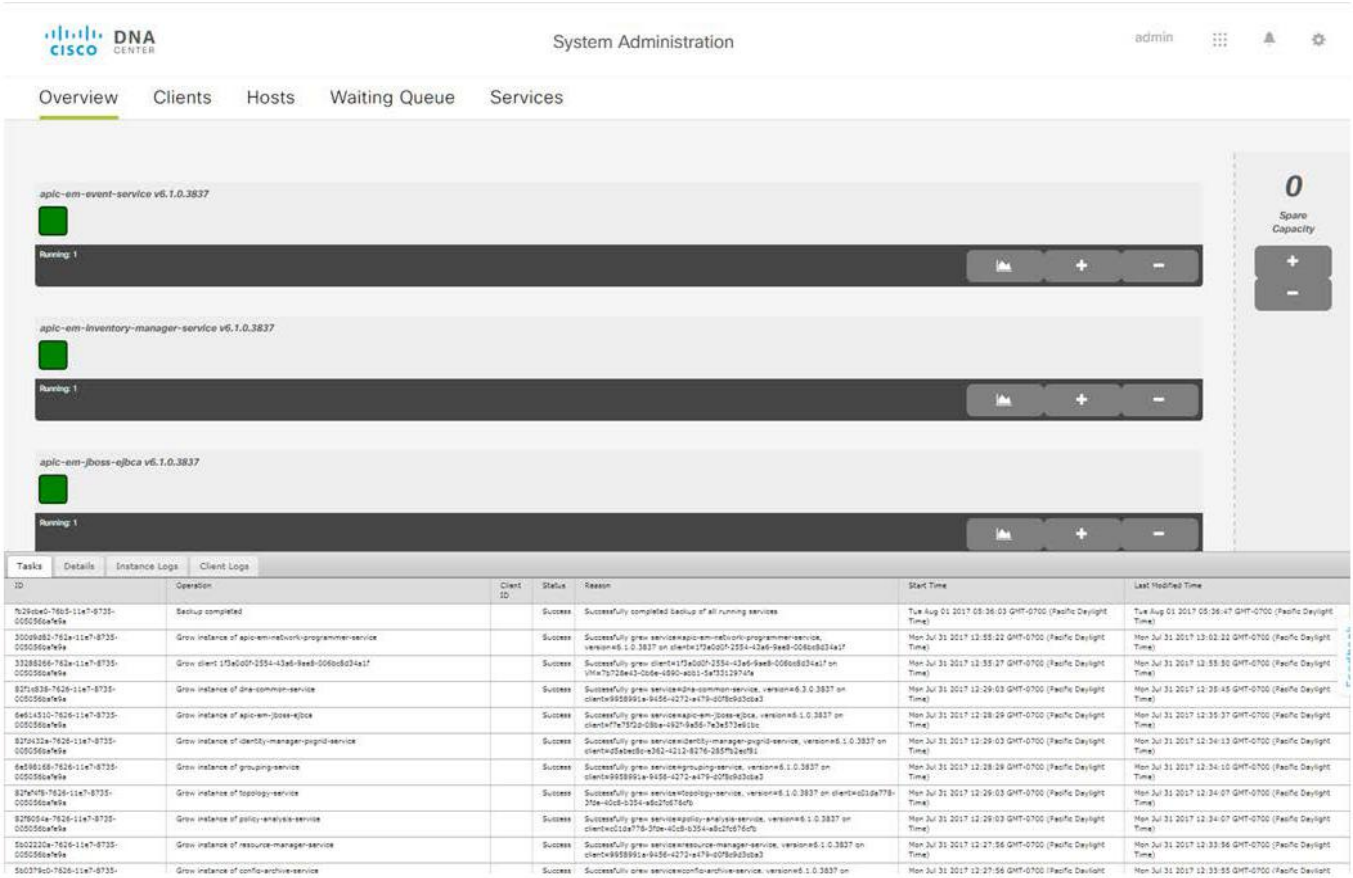


6. DNA Center 내의 다른 링크를 살펴보십시오. 예를 들어 시스템 설정 페이지는 시스템 백업, Restore 뿐만 아니라 DNA Center 시스템이 다른 플랫폼, 사용자 및 응용 프로그램과 통합되는 방법을 제어합니다.

7. DNA Center 를 사용하는 동안, 화면 오른쪽 상단에 있는 애플리케이션 (Apps) 버튼을 클릭하여 응용 프로그램에서 홈 페이지로 쉽게 이동할 수 있습니다. 또한 Cisco 로고 옆에 있는 DNA CENTER 를 클릭하여 이동할 수도 있습니다.



8. DNA Center 에 처음 로그인 할 때 **System administration** 페이지를 확인하여 모든 응용 프로그램이 정상적으로 실행 중임을 나타내는 녹색으로 표시되어 있는지 확인하십시오. 응용 프로그램이 시작되지 않은 경우는 녹색으로 바뀔 때까지 DNA center 사용을 잠시 멈추십시오.



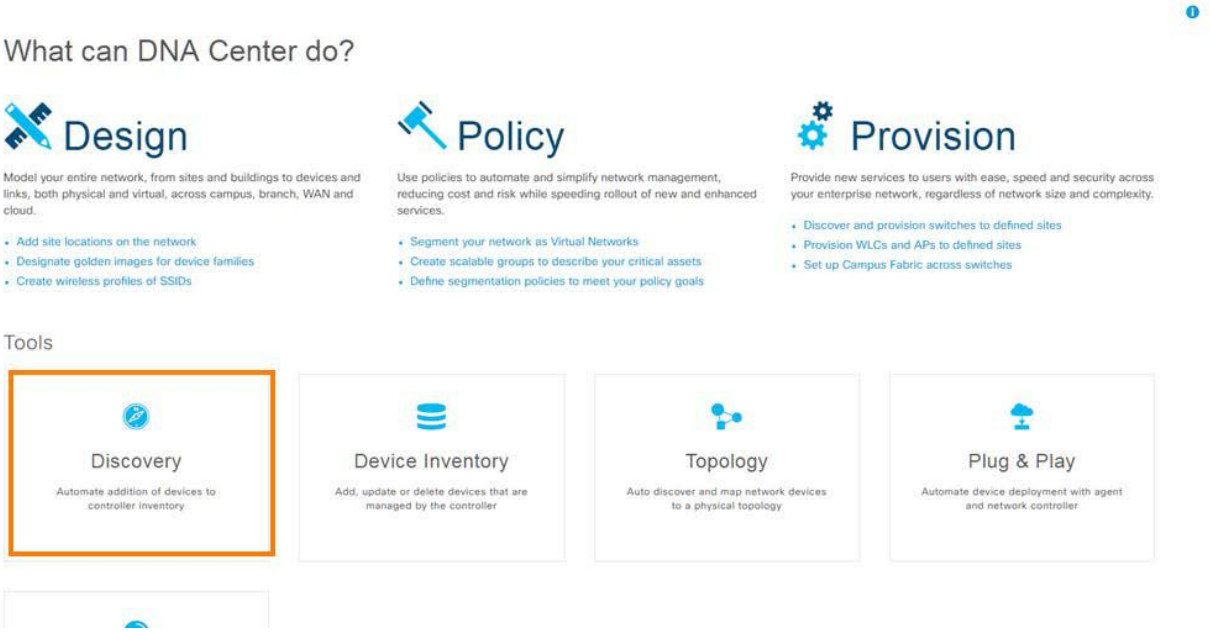
노트: oss-nbl-service 및 resource-access-test-service 애플리케이션은 실행되지 않더라도 문제가 없습니다

시나리오 2. Lab 장치 탐색(Discovery)

DNA Center 에서 Discovery 도구는 CDP 또는 IP 주소 범위를 사용하여 Underlay 장치를 찾는데 사용됩니다. Discovery 프로파일 구성시 사용자는 Design 응용 프로그램에 정의되어 있는 자격 증명을 활용할 수 있습니다 (이후 세션 참조).

스텝:

1. DNA Center 홈페이지로 이동하려면 앱 아이콘을 클릭하십시오.
2. 홈페이지에서 **Discovery** 를 선택하십시오.



3. Discovery 프로파일을 작성하고 실행하기 전, 랩에서 스위치에 설정된 Crypto 및 IP 디바이스 트래킹 (IPDT) 구성을 잠시 살펴보십시오. 스위치 프로파일은 워크 스테이션 데스크탑의 MTPuTTY 에 있습니다. **MTPuTTY 를 열고 Putty Sessions** 세션을 확장하십시오. 장치에 접속하려면 해당 장치를 더블 클릭합니다.
4. 세대의 SD-Access 스위치에 접속하여 다음 명령을 실행하십시오. (C3850-10g-1, C3850-2, C3850-1-stack).

```
show run | inc crypto
show run | sec IPDT
```

노트: 각 스위치에 Crypto 및 IPDT 설정이 적용되어 있습니까? 나중을 위해 Crypto 및 IPDT 설정 내용은 기억해 두십시오.

5. 본 데모에서 사용하는 EFT (Early Field Trial) 코드 버전의 SDA 랩은 Discovery 작업이 수행되기 전 Fabric Border Node 에 BGP 가 구성되어 있어야 합니다. (향후 General 버전에서는 필요하지 않음). 이 실습에서 C3850-10g-1 은 Fabric Border 노드이므로 **show run | sec bgp** 명령을 사용하여 BGP 프로세스가 AS 번호 65004 로 구성되었는지 확인하십시오. 이 설정이 없는 경우 아래의 정보를 입력하십시오

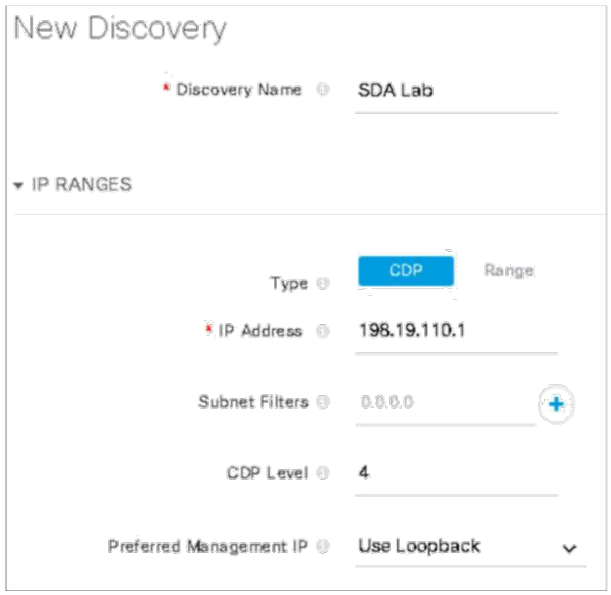
```
C3850-10g-1#conf t
C3850-10g-1(config)#router bgp 65004
C3850-10g-1(config)#end
C3850-10g-1#wr mem
```

6. Discovery Name 을 SDA Lab 으로 지정한 후 아래의 내용을 **IP Ranges** 섹션에 입력하십시오.

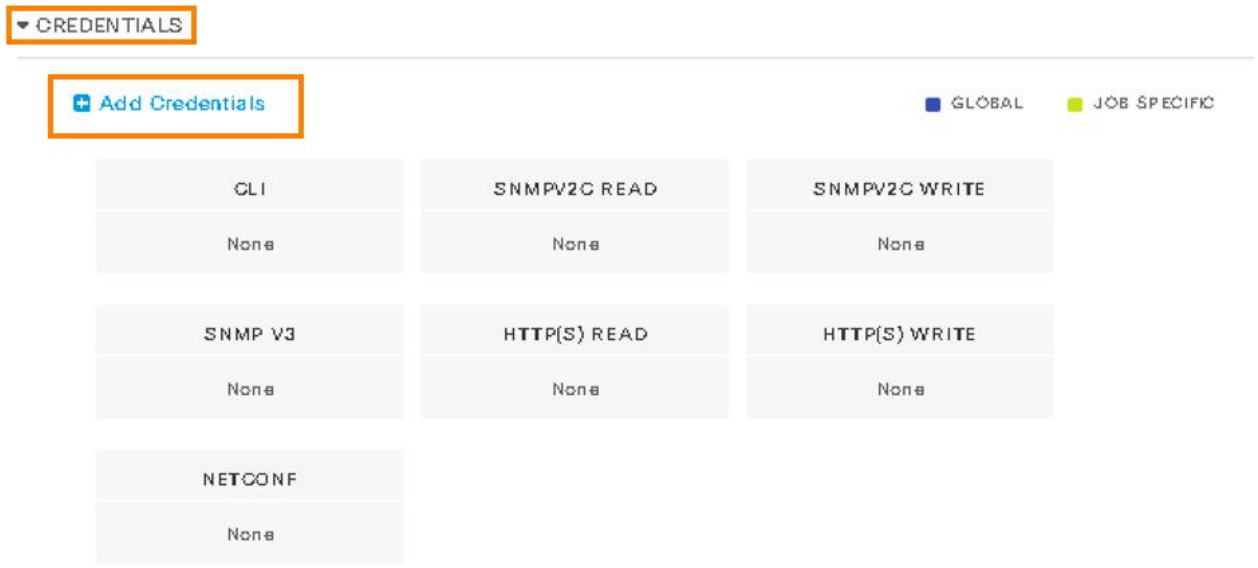
- IP Address: 198.19.110.1
- Subnet Filters: 미입력
- CDP Level: 4
- Preferred Management IP: Use Loopback

노트: DNA Center 가 접속하는 IP 주소는 각 스위치들의 L3 인터페이스 또는 Loopback 입니다. 이 Lab 은 C3850-10g-1 의 Loopback 인터페이스를 사용합니다.

노트: 이 시나리오는 Lab 이 복잡하지 않기 때문에 Discovery 프로세스를 빠르게 하기 위해 CDP Level 4 를 이용합니다.



7. 자격 증명(Credentials)을 펼친 뒤 **Add Credentials** 을 클릭합니다.

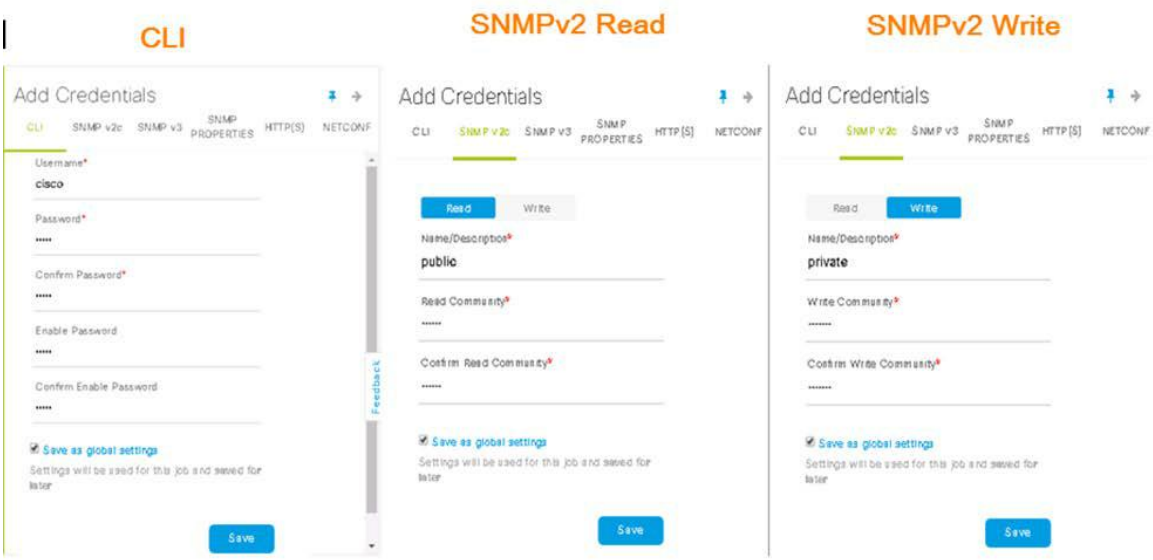


8. 자격 증명 추가 화면이 페이지의 오른쪽에 표시됩니다. 아래 표에 있는 CLI 및 SNMPv2c 의 자격증명 정보를 이용하십시오.

테이블 4. 정보

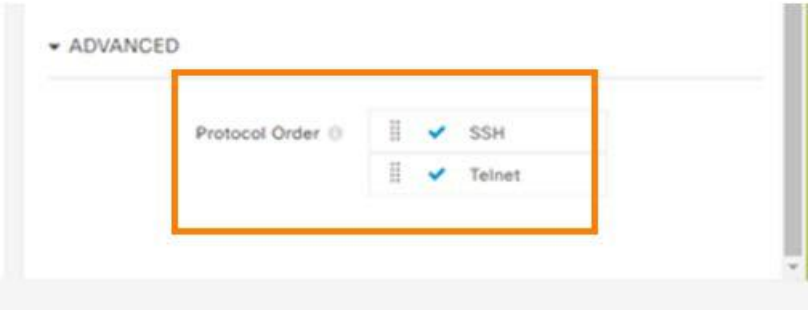
CLI 크리덴셜 정보	
Username	cisco
Password	C1sco12345
Enable Password	C1sco12345
SNMPv2 RO	public
SNMPv2 RW	private

9. 각 옵션에 있는 **Save as global setting box** 에 체크 하십시오. CLI, SNMP Read 및 SNMP Write 정보를 입력하십시오. 정보 입력 후 **Save** 를 클릭합니다.

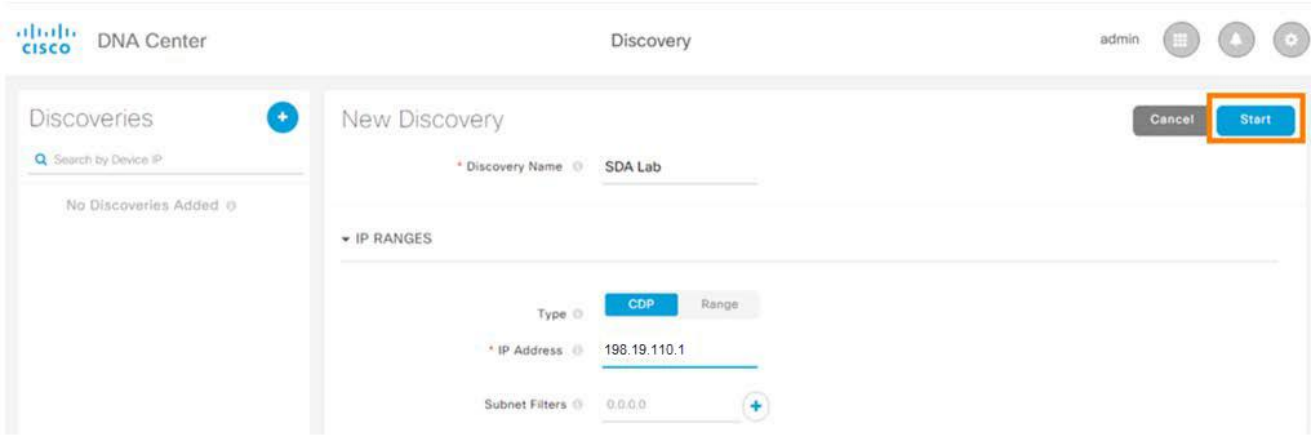


10. 입력된 정보가 전달되면, 입력된 정보가 페이지 중앙에 표시됩니다. Box 의 파란색 부분은 해당 정보가 Global setting 임을 나타냅니다. 만약 녹색으로 표시되면 Global 설정이 아닙니다.

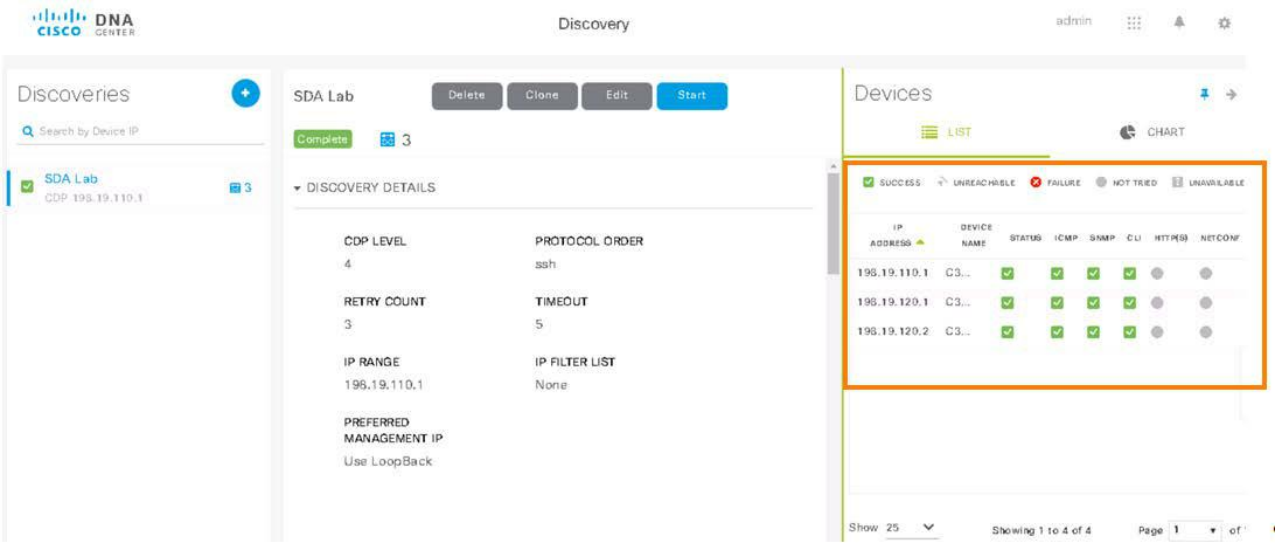
11. 마지막은 SSH 구성이 적용되어 있지 않은 레거시 장비를 위한 Discovery 프로토콜로 Telnet 활성화합니다. 이렇게 하려면 페이지를 아래로 스크롤하여 **Advanced** 섹션을 엽니다. **Telnet** 을 선택하십시오.



12. 오른쪽 상단 구석의 **Start** 를 클릭하십시오. Discovery 가 시작되면 페이지에 검색 설정과 세부 정보가 표시됩니다. 명명된 Discovery 위에 진행 표시가 나타납니다. 이 작업은 몇 분 정도 걸릴 수 있으니, 잠시 기다리십시오.



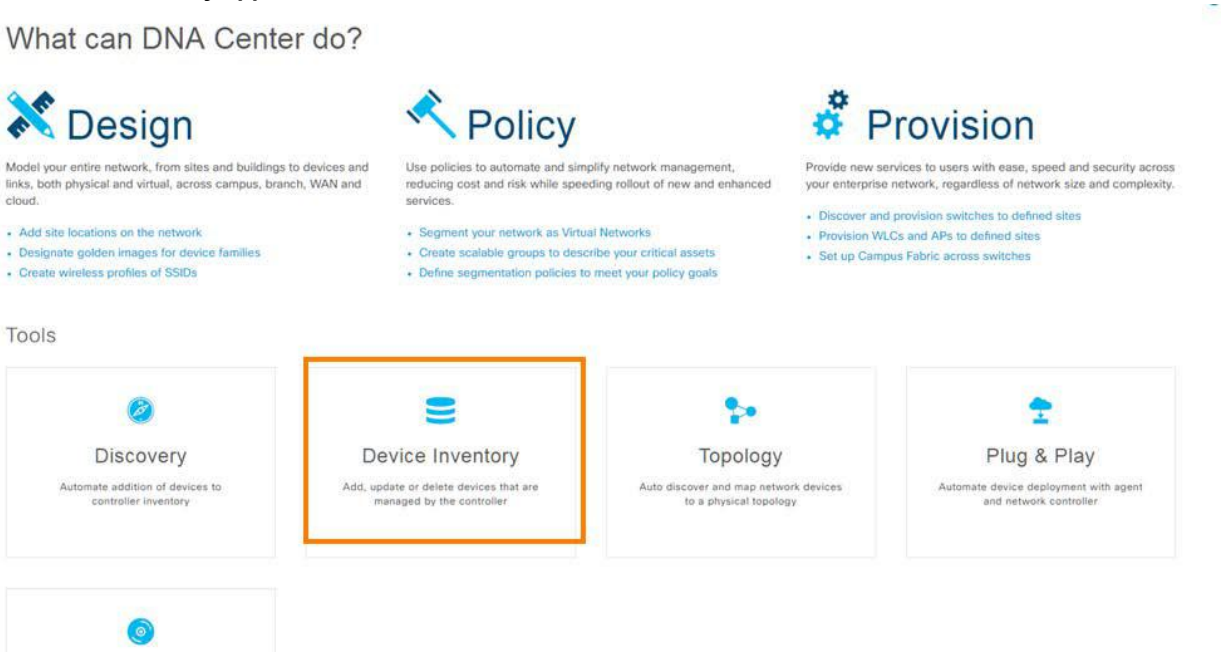
13. 잠시 후, 화면 오른쪽에 발견 된 장치가 표시됩니다.



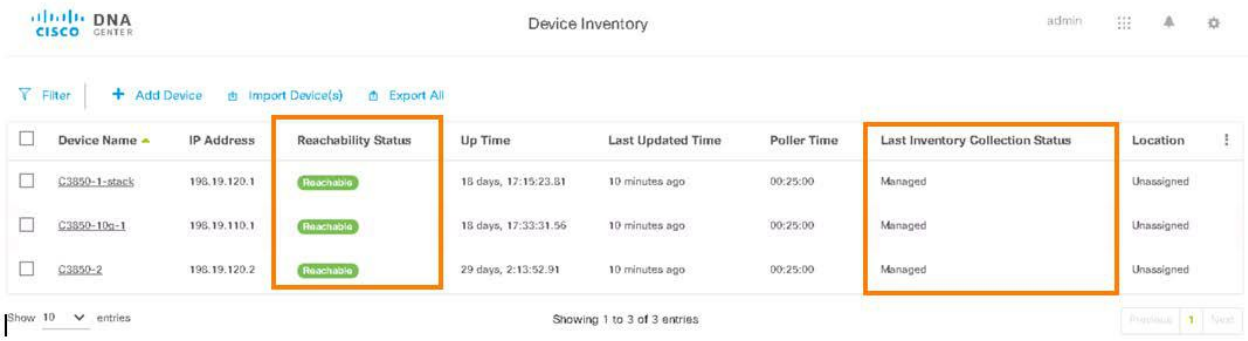
시나리오 3. 인벤토리 앱 (Inventory App)

스텝:

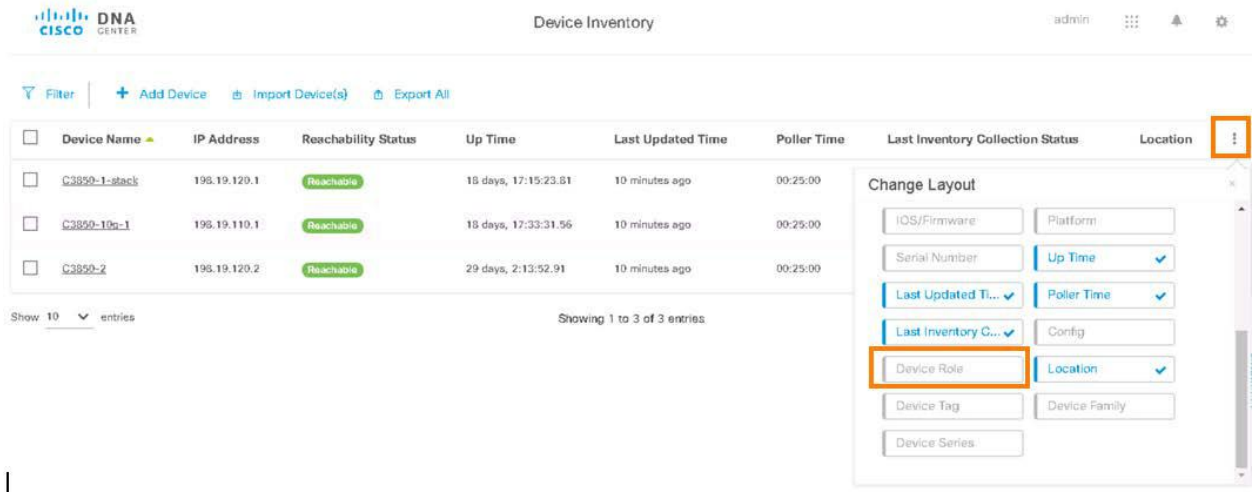
1. 장치가 발견되면, **Apps** 버튼을 클릭해서 DNA Center 홈페이지로 이동합니다. 그 다음 랩 장치를 보기 위해 **Device Inventory app** 을 열어주십시오.



2. Device Inventory (장치 인벤토리) 페이지로 들어가면 모든 장치의 **Device Status** 가 **Reachable** 로 설정되어 있어야 합니다. 그리고 **Last Inventory Collection Status** 가 **Managed** 로 설정되어 있어야 합니다.



3. Device Roles(장치 역할)은 DNA Center 구성도 맵에서 장치를 포지셔닝하기 위해 사용됩니다. **Layout** 설정을 사용하여 **Device Role** 열을 테이블에 추가한 뒤 각 장비의 역할을 수정합니다.



I

4. Device Role 열에서 C3850-10g-1 으로 이동하여 역할을 Border Router 로 변경합니다. 선택하려면 아래로 스크롤해야 할 수도 있습니다.
5. **C3850-1-stack** 및 **C3850-2** 가 Access Role 로 되어있는지 확인하십시오.
6. 진행하기 전에 Catalyst 스위치 구성을 다시 한 번 살펴봅니다. Discovery 진행 중, DNA Center 가 변경한 스위치 설정을 확인합니다.

```
C3850-2#show run | i crypto
crypto pki trustpoint 198.18.129.100 crypto
pki certificate chain 198.18.129.100
```

노트: 이 Certificate 은 DNA Center 가 각 장치와 신뢰할 수 있는 연결을 수립하기 위한 용도로 만들어졌습니다. 이 Certificate 구성이 Discovery 작업 이전의 스위치 구성에 있었습니까?

```
C3850-2#show run | sec IPD
device-tracking policy IPDT_MAX_10
 limit address-count 10
 no protocol udp
 tracking enable
 device-tracking attach-policy IPDT_MAX_10
 device-tracking attach-policy IPDT_MAX_10
<snip>
```

노트: IPDT (IP 장치 추적)는 연결된 호스트를 추적하는데 사용됩니다. 이는 유니캐스트 ARP 프로브를 통해 수행되며 다양한 서비스에 이용됩니다. SD-Access 의 경우에는, Cisco Trustsec, MAB (MAC 인증 바이패스) 및 802.1x 세션 관리에 사용됩니다. Discovery 작업 이전에 스위치에 IPDT 구성이 있었습니까?

여러분은 DNA Center 가 제공하는 강력한 오케스트레이션 기능을 간단히 접했습니다. 이 Lab 에는 비록 소수의 장치 밖에 없지만, DNA Center 를 이용하면 수백 또는 수천 대의 장치로 구성된 엔터프라이즈 환경에서 오케스트레이션을 수행할 수 있습니다.

스위치의 구성 확인이 끝났으면 Apps 버튼을 클릭하여 다음 내용의 진행을 위해 DNA Center 홈 페이지로 이동하십시오.

시나리오 4.DNA Design Center 이용하기

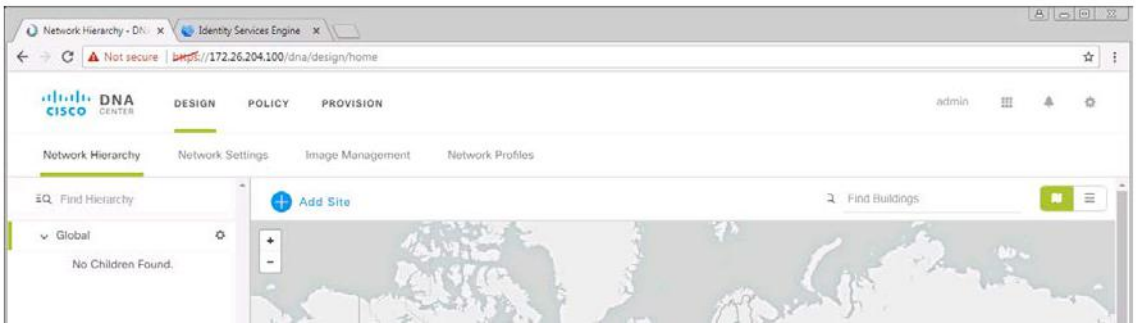
DNA Center 는 다양한 사이즈 및 규모의 고객 인프라환경에 물리적 장소와 인프라에서 공통적으로 사용하는 리소스를 손쉽게 정의할 수 있도록 도와주는 디자인 애플리케이션을 제공합니다. 이 기능을 통해 복잡한 네트워크에 속해있는 여러 장비에 대한 반복적인 리소스 할당 및 정의 작업을 수행할 필요 없이 직관적인 방식으로 계층적 설계를 수행할 수 있습니다.
계층 구조를 통해 고객은 서비스 용도에 따라 글로벌 및 지역적 표준 구성이 가능하도록 유연성을 확보할 수 있습니다. 예를 들어, 고객은 글로벌 DNS 및 NTP 서비스는 글로벌로 동일하게 설정하고 각각의 지역 또는 로컬 사이트에는 자체 DHCP 및 / 또는 AAA 서비스를 운영할 수 있습니다. 이 방식은 장비에 대한 자격 증명, 무선 SSID 및 IP 서브넷에도 적용됩니다. 모든 구성은 결국 전 세계적으로, 지역적으로, 로컬 형식으로 또는 이들을 혼합하여 구성할 수 있습니다.
이 내용은 뒤에 진행될 데모를 통하여 여러분이 사이트를 생성하고 관련된 네트워크 설정을 해봄으로써 DNA Center 의 Design 애플리케이션에 친숙해지도록 합니다.

스텝:

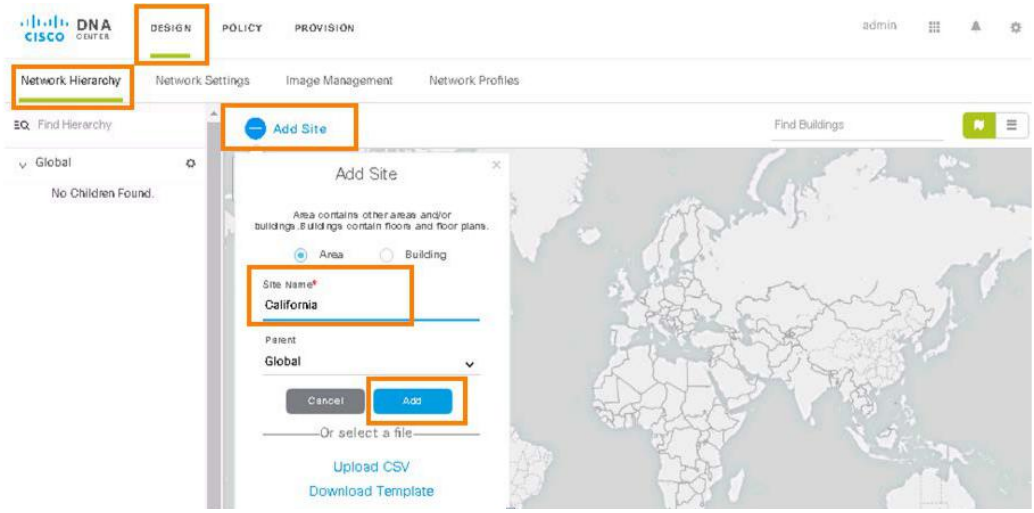
사이트 및 건물(Building) 생성하기

1. 시작하기 위해 **Design app** 을 선택합니다. **Design app** 으로 이동하면 세계지도가 보이고 화면 왼쪽에는 사이트의 계층 구조가 표시되어 있습니다.

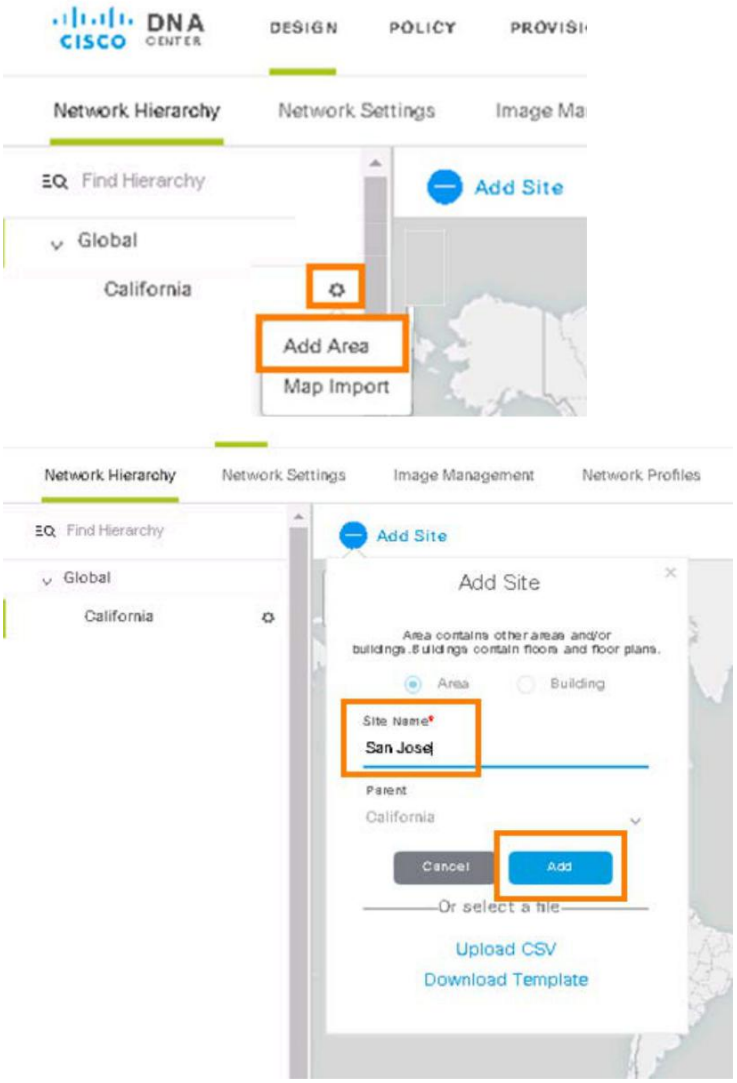
노트: 브라우저에 세계지도가 표시되도록 하기 위해서는 인터넷 연결이 필요합니다.



2. **California** 사이트를 만들기 위해 **Add Site** 를 클릭한 뒤 **California** 입력 후 **Add** 를 클릭합니다.



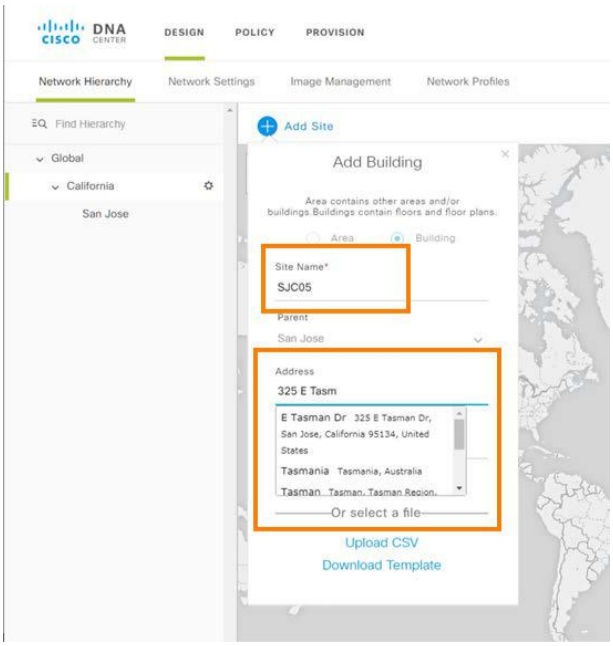
3. 다음으로 California 옆에 있는 톱니바퀴 를 클릭하여 다른 사이트를 만듭니다. **Add Area** 를 선택하십시오. 상위 Parent 노드가 California 인지 확인하십시오. 사이트 이름을 San Jose 로 지정한 다음 **Add** 를 클릭하십시오.



4. California 를 열고 San Jose 옆에 있는 톱니바퀴 아이콘 을 선택하여 네트워크 장치가 설치될 장소 추가를 위해 **Add a Building** 을 클릭합니다. 건물 이름은 SJC05 로 합니다.

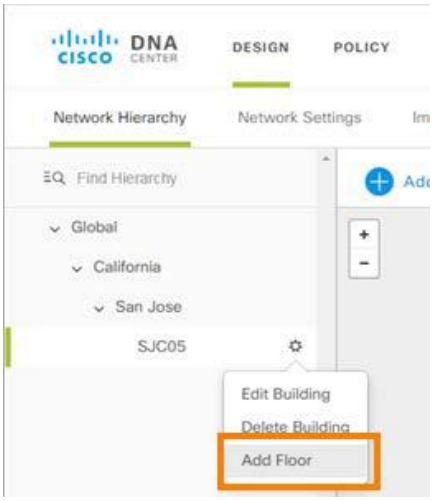
5. 빌딩 주소는 **325 E Tasman** 을 입력하십시오. 주소를 입력하면 Design App 에서 현재 등록되어 있는 실제 주소에 가장 가까운 주소 결과가 나타나는 것을 볼 수 있습니다. 325 E Tasman Dr 이 나타나면 해당 주소를 선택하십시오. 기존에 등록되어있는 주소 선택시 위도와 경도 좌표가 자동으로 표시된다는 장점이 있습니다.

6. San Jose 사이트에 SJC05 건물을 추가하기 위해 **Add** 를 클릭하십시오. 추가되면 지도가 해당 건물을 Zoom in 하여 확대됩니다.



노트: 다음 7-10 단계는 참고만 하십시오. 건물의 층 정보 및 평면도를 추가하는 방법을 보여줍니다. 이 시나리오에서는 평면도를 실제로 불러오는 실습은 포함하지 않기 때문에 기능 및 워크플로우만 설명합니다.

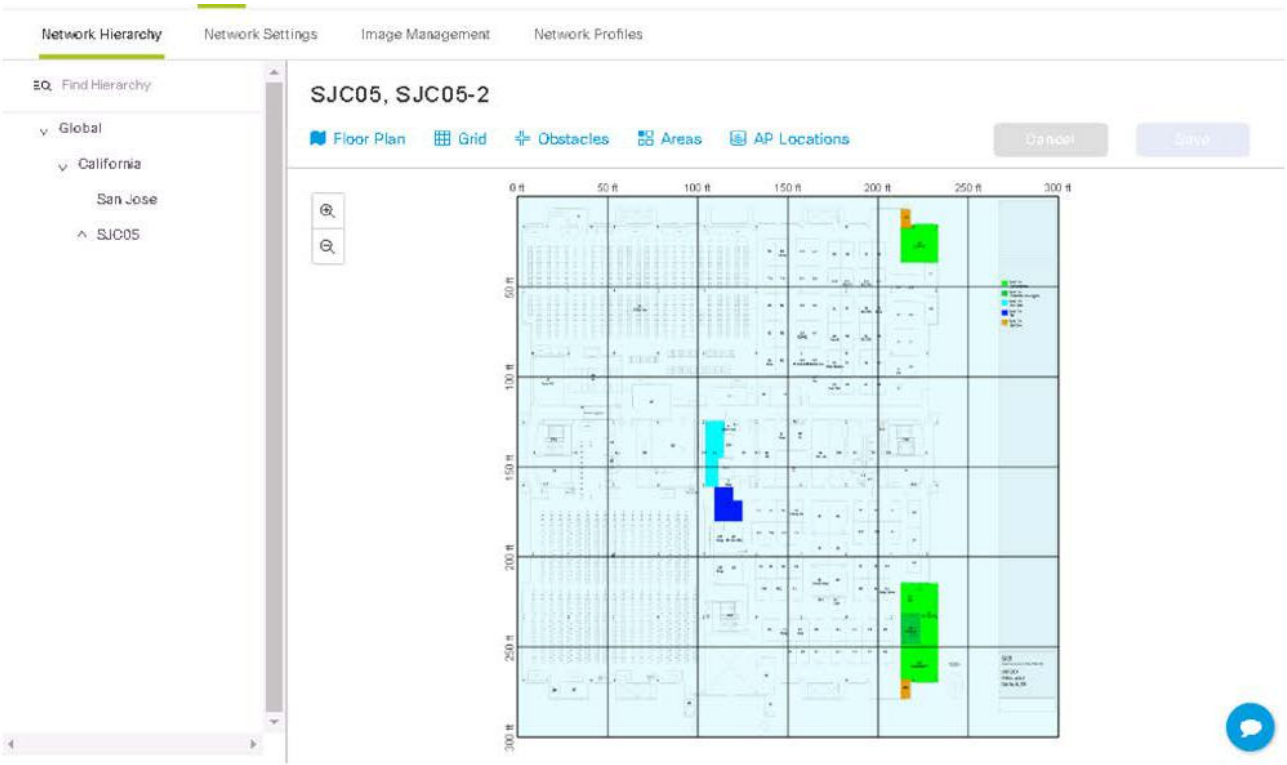
7. San Jose 를 확장하고 SJC05 옆에 있는 톱니바퀴 버튼을 사용하여 건물의 층을 추가합니다. 이름을 **SJC05-1** 로 지정하고 옆의 평면도 정보를 이용하십시오: (Width) 너비– 300, 길이(Length)– 300, 높이(Height)– 15, 층 (Floor #)– 1.



8. 층이 생성되면 평면도를 추가할 수 있습니다. PNG, JPG, GIF 또는 CAD 파일을 평면도로 불러올 수 있습니다.

9. 1 층과 동일한 면적의 2 층 SJC05-2 를 만듭니다 (면적은 동일하며 #는 2 가 됩니다).

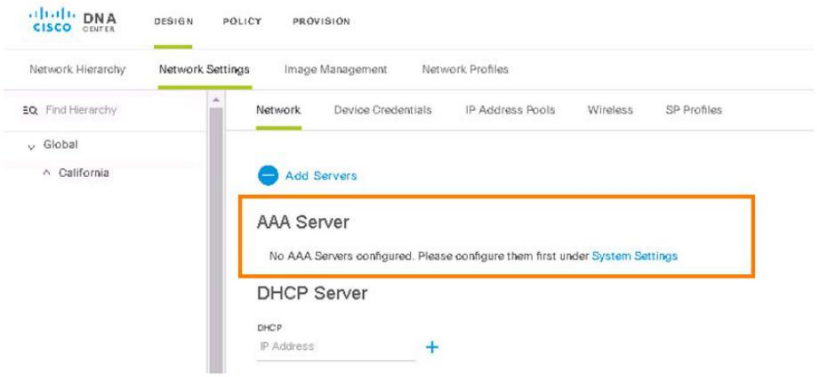
10. 평면도를 불러오게 되면, 아래와 같은 내용이 표시됩니다.



노트: DNA Center 에서는 Design app 의 네트워크 설정을 통해 인프라 내에서 사용하는 공용 리소스 및 설정을 저장할 수 있습니다. 앞서 설명했듯이 기업 내부에서 사용하는 속성 정보를 저장하면 DNA Center 에서 재사용 할 수 있습니다.

11. Network Hierarchy 탭에서 메뉴 바를 클릭하여 **Network Settings** 로 이동할 수 있습니다.

12. **Network Settings** 탭으로 이동하면 전체 네트워크 환경에 대한 일반설정 목록이 나타납니다. SD-Access 는 AAA, DHCP 및 DNS 서버 구성을 필요로 합니다. 기타 서버 (NTP, NetFlow 컬렉터, SNMP 트랩, Syslog)도 추가 할 수 있습니다.

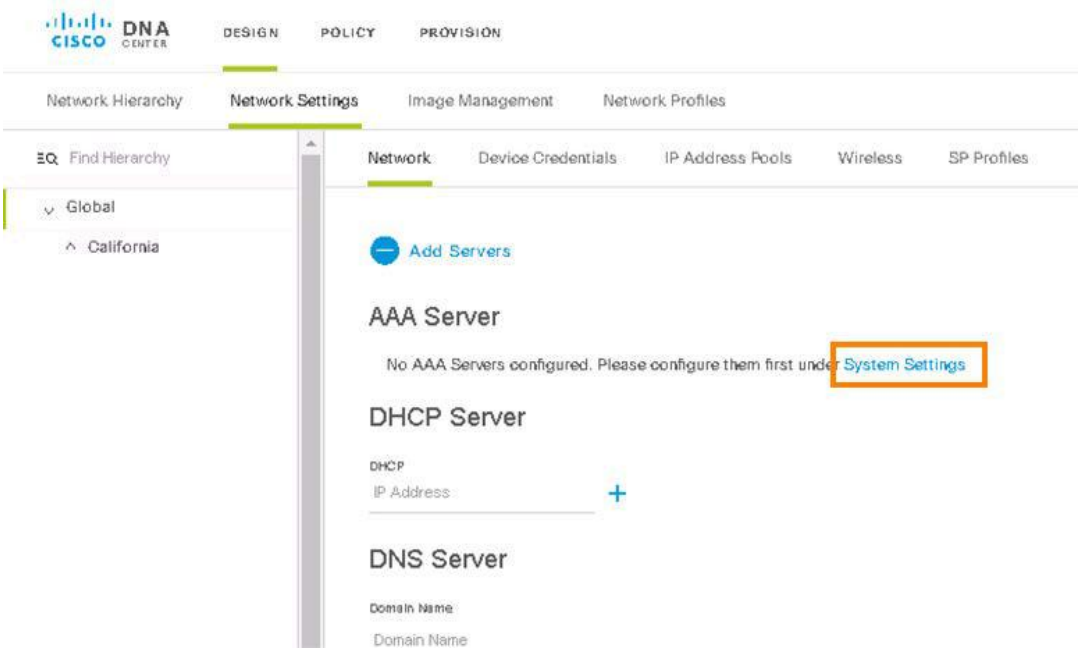


노트:이 메시지는 ISE 가 아직 DNA Center 에 통합되지 않은 경우 나타납니다.

DNA Center - ISE 통합

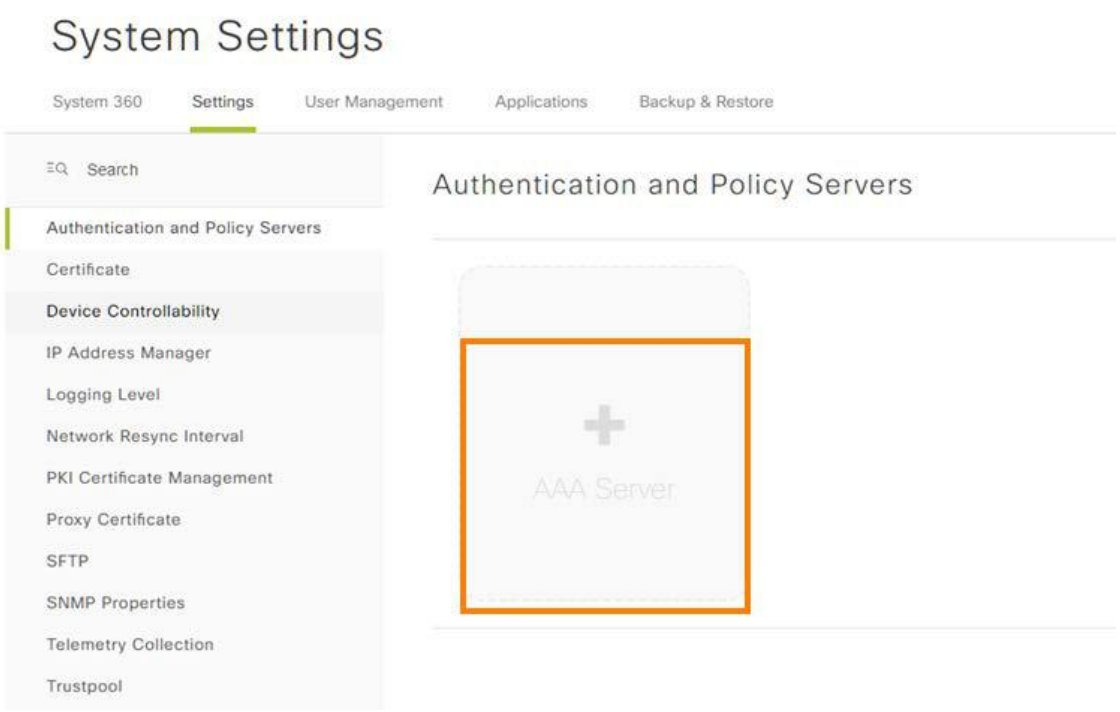
Cisco 플랫폼 익스체인지 그리드 (이하 pxGrid)는 IT 인프라에 속한 서로 다른 구성요소들을 하나로 연결시켜주는 멀티 벤더, 크로스 플랫폼 네트워크 시스템입니다. Cisco pxGrid 는 SSL 인증서를 통한 보안성 있는 API 연결을 제공합니다. DNA Center 는 보안적 관점에서 이용자가 DNA Center 와 ISE 통합을 손쉽게 수행할 수 있도록 인증서 프로세스를 자동화했습니다.

1. DNA Center 의 AAA 서버에 ISE 를 추가하기 위해 **Systems Settings** 를 클릭하십시오.



2. 클릭하면 **Authentication and Policy Servers** 화면으로 이동합니다.

3. **+ AAA Server** 를 클릭하면 설정화면이 표시됩니다.



4. AAA / ISE 서버 1 세부 정보를 채웁니다. 정보 입력 필드 표시를 위해 Cisco ISE 슬라이더를 옆으로 이동하십시오. (활성화 시키면 슬라이더 부분이 파란색으로 바뀜). 아래의 정보를 사용하십시오.

- ISE IP address: **198.18.133.27**
- Shared Secret: **C1sco12345** (장치와 ISE 간에 사용)
- Username: **admin**
- Password and Confirm Password: **C1sco12345**
- FQDN: **sda-ise.dcloud.cisco.com**.

노트:DNS Resolve 용도로 지금 필요하지는 않지만 일단 **ISE 의 실제 FQDN 과 일치시켜야 합니다.**

- Subscriber Name: **dnac**
- SSH key: N/A (필수 아님)

5. **Apply 를** 클릭합니다. 다음 단계로 진행하기 전에 DNA Center 가 연결 설정을 마칠 때까지 기다리십시오. 이 작업은 최대 5 분 정도 걸릴 수 있습니다.

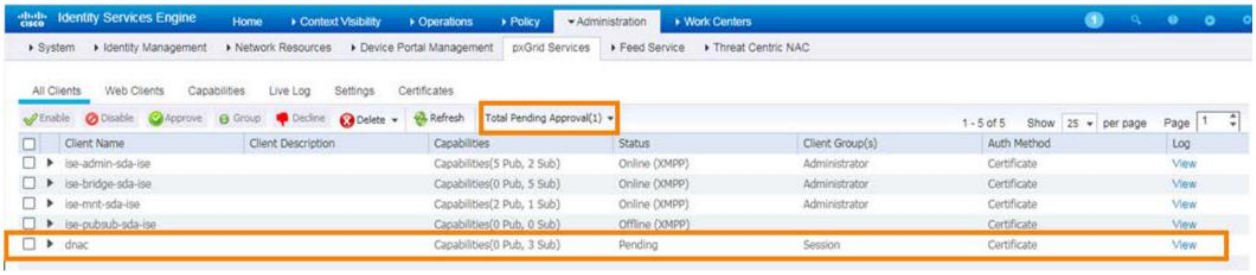
6. ISE 와의 연결 상태 및 Subscriber 확인을 위해 ISE 에 접속합니다. 아래 로그인 정보 및 IP 어드레스 https://198.18.133.27 (ISE 탭은 브라우저에 있어야 함)를 이용해 ISE 에 로그인 하십시오.

   User ID: **admin**

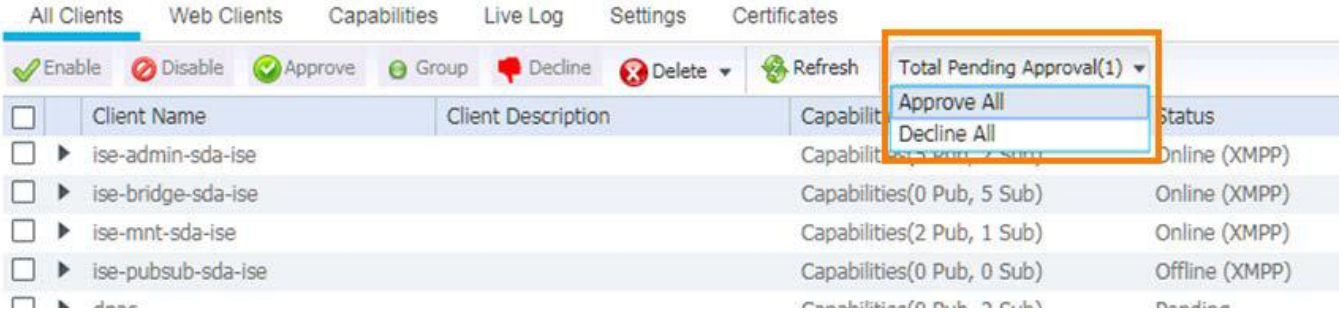
   Password: **C1sco12345.**

7. 인증되면 **Administration > pxGrid Services** 로 이동하십시오. 이 페이지에서 **DNAC Client** 는 Pending 및 Total Pending Approval (1)으로 나타납니다.

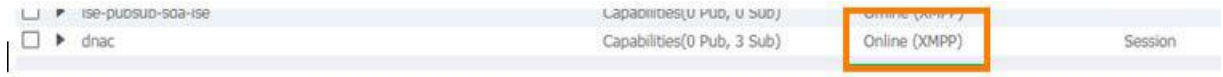
노트: 통합 완료될 때까지 일반적으로 2-5 분이 소요됩니다. ISE 에 로그인 후, 보다 빨리 DNAC Subscriber 확인을 위해 페이지를 새로 고침(Refresh) 합니다.



8. **Total Pending Approval (1) > Approve All** 을 선택하십시오.

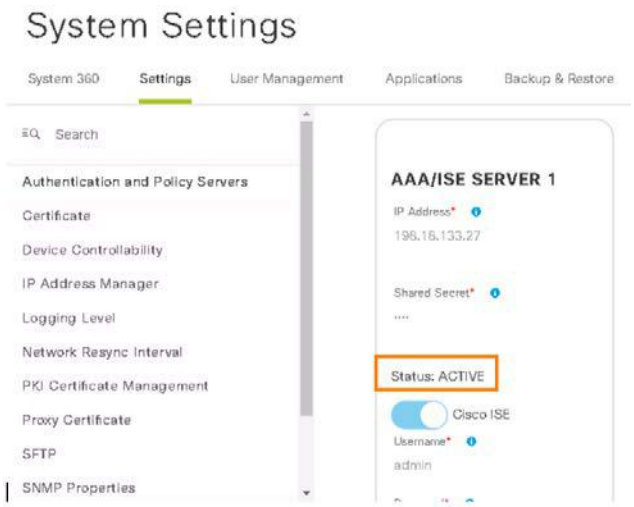


9. 그 다음 DNAC 클라이언트가 온라인 상태(**Online status)**가 됩니다.



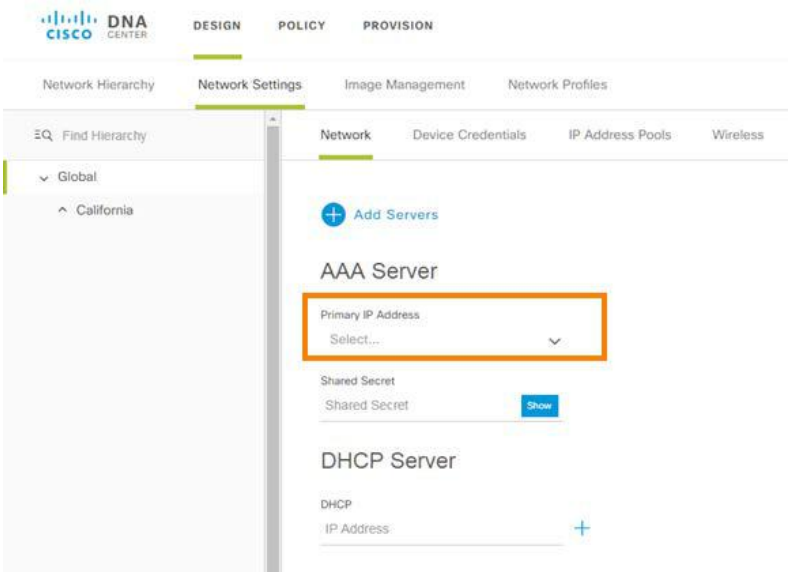
10. 페이지 하단에 온라인으로 연결되었다고 녹색으로 상태가 표시됩니다.

11. DNA Center 페이지에 돌아가 시스템 설정의 AAA / ISE 서버 상태가 **ACTIVE** 로 표시되는지를 확인하십시오.



네트워크 설정

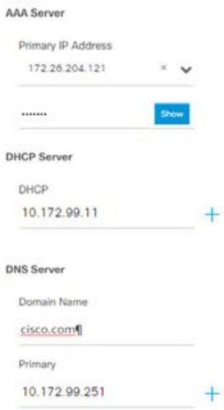
1. **Design > Network Settings** 으로 이동하십시오**.** 여기서 DNA Center 가 AAA 관련 메시지를 표시하지 않아야 합니다. 이는 ISE 와 DNA Center 가 성공적으로 연동되었음을 의미합니다. AAA 서버의 아래쪽 화살표를 클릭하여 이를 확인할 수 있습니다.



2. 이 화면을 통해 아래 테이블 5 의 서버 정보를 확인하십시오. AAA 서버는 ISE 정보이며, DHCP 또는 DNS 는 지금 사용하지는 않지만 어드레스는 구성되어 있습니다.

테이블 5. 서버 정보

서버	IP 주소	속성
AAA (ISE)	198.18.133.27	Shared Secret: C1sco12345
DHCP	10.172.99.11	
DNS	10.172.99.251	Domain name: cisco.com

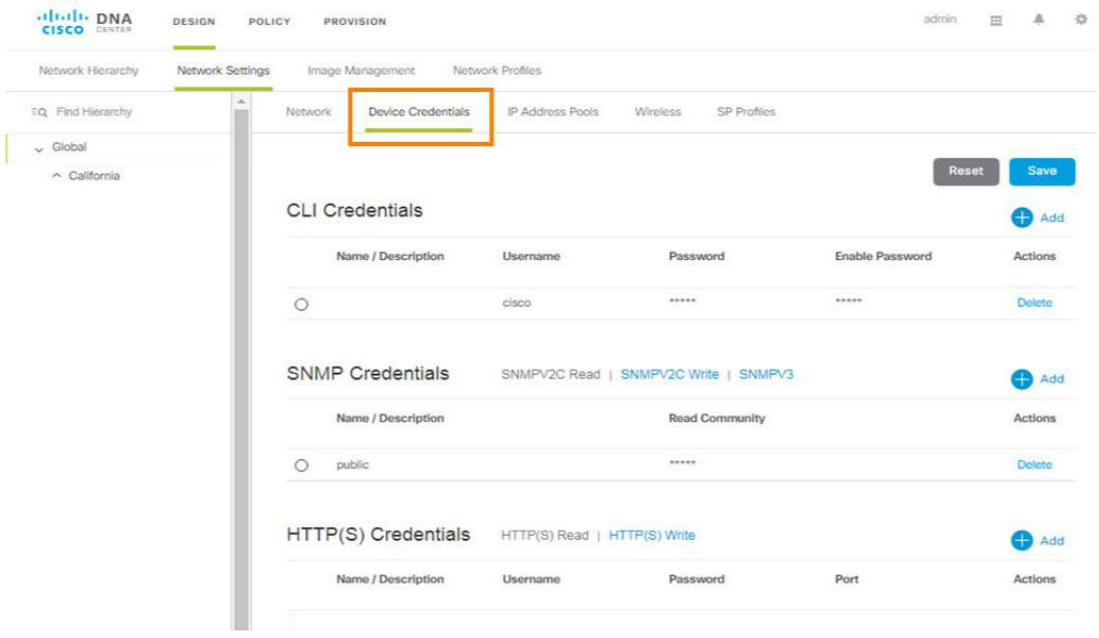


노트: 이 랩에서는 DHCP 및 DNS 서버가 따로 없지만 DNA Center 에 속성값을 입력할 필요는 있습니다.

3. 오른쪽과 같이 정보를 입력 한 후 오른쪽 상단 모서리에 있는 **Save** 을 클릭하십시오.

Device Credentials

1. 다음 단계는 사이트 장비의 자격 증명(Credentials)을 정의합니다. 메뉴 바에서 **Device Credential** 을 선택합니다. 여기에서는 이전에 Discovery 도구에 정의된 Credentials 정보를 보여줍니다. 만약 장비를 추가하고 이에 대한 자격 증명도 추가하려면 이 시점에서 수행할 수 있습니다.

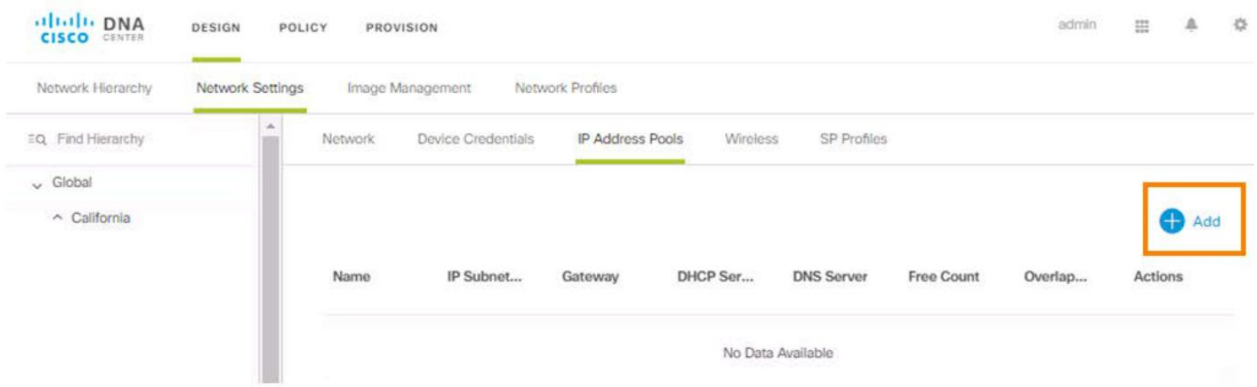


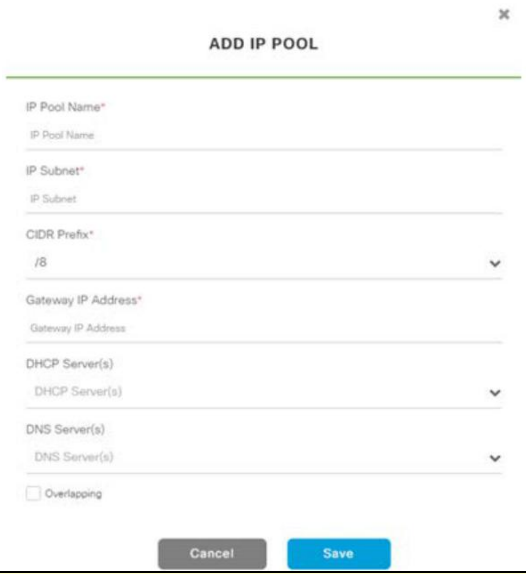
IP Pool 생성하기

DNA Center 는 수동 IP 어드레스 할당 또는 이미 사용중인 IP 어드레스 확인을 위해 Infoblox 와 같은 IPAM(IP 주소 관리) 솔루션과 통합시키는 방식 둘다 지원합니다.

1. 이 랩에서는 IP 어드레스 Pool 을 수동으로 정의합니다. 메뉴 바에서 **IP Address Pools** 을 선택하십시오.

2. **Add** 를 클릭하여 새 IP Pool 을 생성하기 위한 대화 박스를 엽니다.





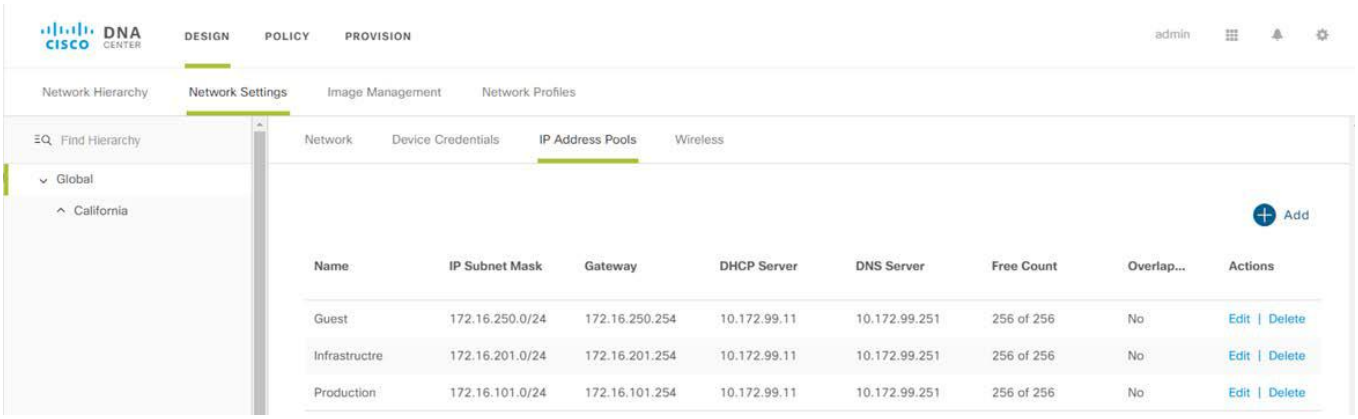
노트: **Overlapping check box 에 체크하지 마십시오**. 이 체크 박스는 네트워크 내에서 중복되는 서브넷(Subnets)을 식별할 수 있게 하여 IP 어드레스가 여러 장소에서 사용될 수 있게 해줍니다.

3. 테이블 6 의 네트워크 설정 정보를 사용하여 랩에 이용할 **3 개의 IP Pool** 을 만듭니다. IP Pool 설정시 이전에 네트워크 설정 부분에서 입력한 DHCP 및 DNS 서버의 정보가 옵션으로 표시되는지를 확인합니다.

테이블 6. 네트워크 설정 정보

이름	IP 서브넷 마스크	Gateway	DHCP 서버	DNS 서버
Production	172.16.101.0/24	172.16.101.254	10.172.99.11	10.172.99.251
Infrastructure	172.16.201.0/24	172.16.201.254	10.172.99.11	10.172.99.251
Guest	172.16.250.0/24	172.16.250.254	10.172.99.11	10.172.99.251

4. 완료되면, **DNA Center** 의 글로벌 **IP Address Pool** 이 아래 정보와 같아야 합니다:



시나리오 5. DNA Center 정책 사용

정책 애플리케이션(Policy App)은 가상 네트워크, 정책 관리, Contract 의 생성 및 관리를 지원하고 Register 기능을 통해 ISE 와 연결되어 확장 그룹(Scalable Group) 생성을 지원합니다. 대부분의 사용자는 SD-Acces 프로비저닝을 수행하기 전에 SD-Access 의 정책(가상 네트워크 및 Contract) 설정을 먼저 수행하려 할 것입니다.

이 섹션에서는 DNA center 의 Policy App 을 사용하여 Overlay 네트워크를 세그멘테이션합니다. 이 과정은 Overlay 네트워크를 여러 개의 독립적인 가상 네트워크로 만듭니다. 기본적으로 하나의 가상 네트워크에 속해있는 모든 네트워크 장치 또는 이용자는 같은 가상 네트워크의 다른 사용자 및 장치들과 통신할 수 있습니다. 그리고 서로 다른 가상 네트워크간의 통신은 일단 트래픽이 패브릭 경계(Fabric Border)를 벗어난 뒤 다시 되돌아와야 하며 일반적으로는 외부 방화벽이나 라우터를 거치게 됩니다.

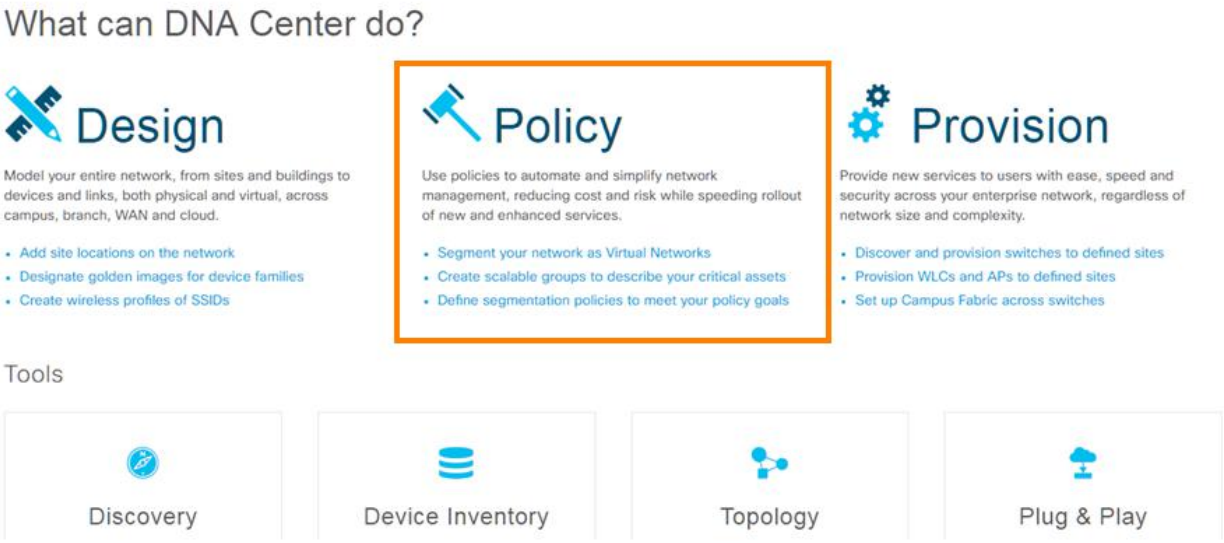
이 내용에서는 DNA Center 의 Policy App 을 통해 가상 네트워크, 확장 그룹(Scalable Group) 및 확장 그룹간의 정책 적용을 위해 사용하는 사용자 지정 Contract 를 생성해봄으로써 여러분이 Policy App 에 익숙해지도록 합니다. SD-Access 환경에서의 다계층 네트워크 세그멘테이션이란 Policy App 이 해당 기능을 오케스트레이션하는 것으로 이해하면 됩니다. 또한 pxGrid 를 이용한 ISE-DNA Center 통합이 SD-Access 아키텍처에서 어떻게 유연성과 효율성을 가져다 주는지에 대해 보다 쉽게 이해할 수 있습니다.

스텝:

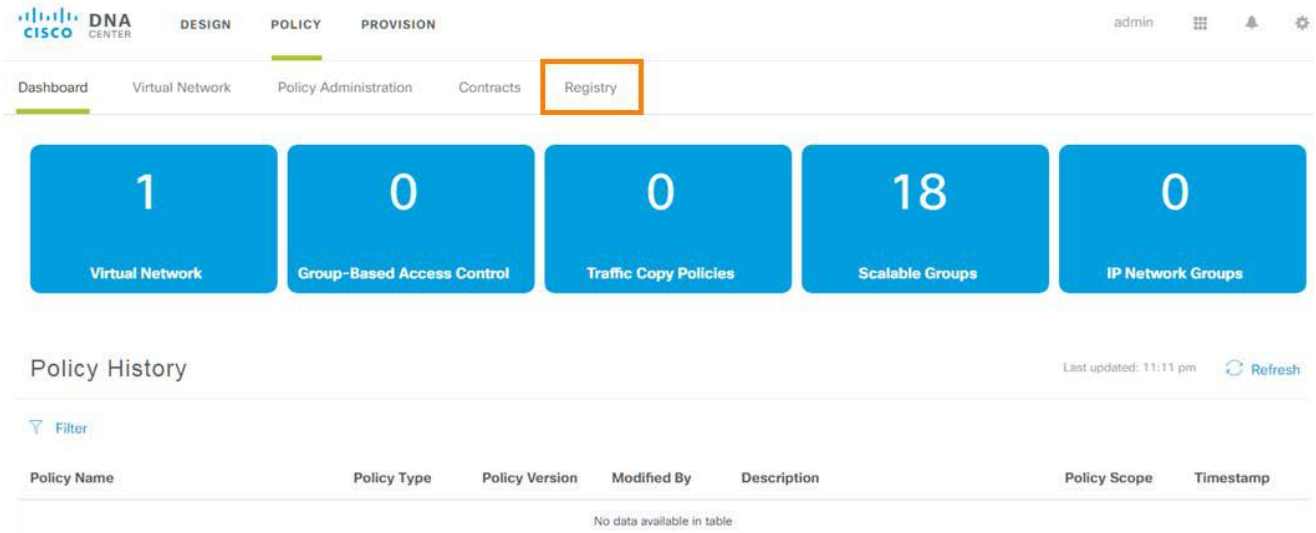
사용자 그룹을 위해 확장 그룹 태그(Scalable Group Tag)를 정의

사용자 그룹은 SGT (Scalable Group Tag)와 연동됩니다. SGT 는 네트워크 전체를 통해 전달되며 Cisco DNA 환경에서 네트워크 접근 정책을 수행하기 위한 기본입니다. (여러분들은 아마 Cisco Trustsec 과 관련해 Security Group Tag 에 대해 들어봤을 것입니다. Scalable Group Tag 는 Security Group Tag 의 또 다른 이름입니다).
이 시나리오 연습이 가져다 주는 Key 목적은 아직 ISE 에 익숙하지 않은 사람들이 DNA Center 를 통해 손쉽게 ISE 에 접근하여 SGT 를 생성할 수 있도록 하는 것입니다.

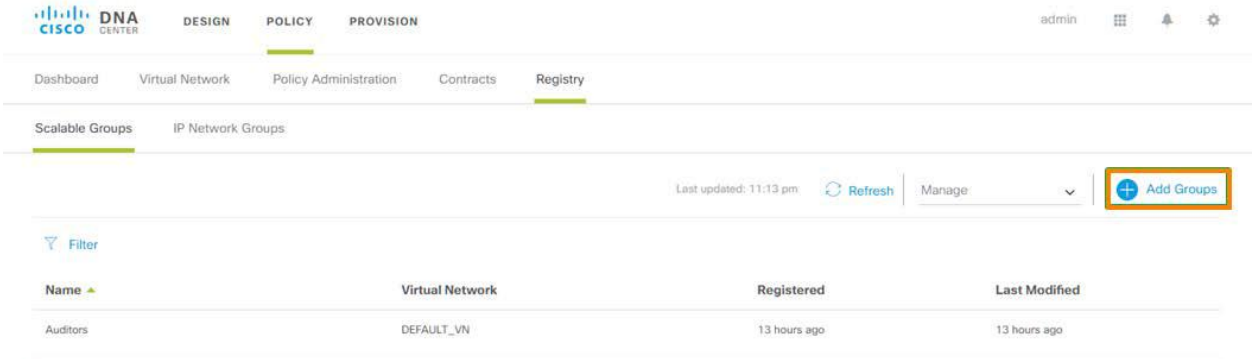
1. **Apps** 버튼 을 클릭하여 DNA Center 홈 페이지로 이동한 다음 **Policy** App 을 클릭하십시오.



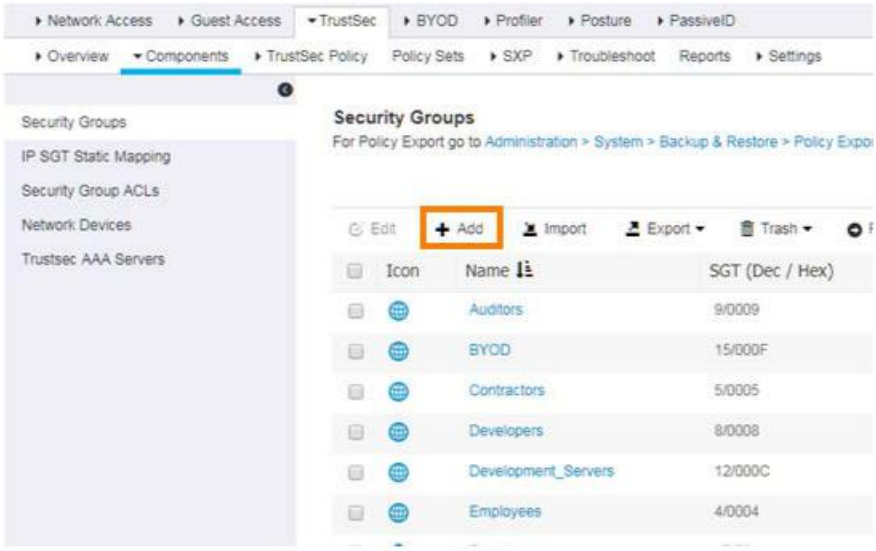
2. **Policy** App 에서는 정책 및 정책과 관련된 액션 히스토리 대시보드를 볼 수 있습니다. Scalable Groups 이 몇개 있는지 확인 하십시오. Policy 페이지에서 **Registry** 를 클릭합니다.



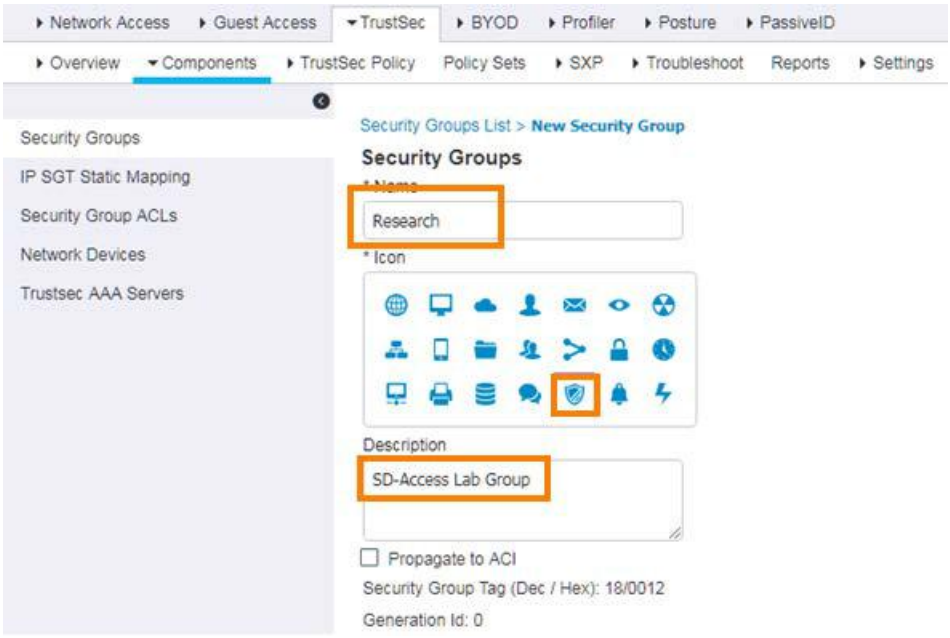
3. ISE 에서 내려 받은 디폴트 확장 그룹 태그를 확인합니다. 그룹을 탐색하고 Research 라는 그룹이 있는지 확인하십시오. 찾을 수 없습니까? 그렇다면 **Add Groups 를** 클릭하십시오.



4. 브라우저에서 ISE 연결을 위해 새로운 탭이 열립니다. 로그인 필요한 경우, admin / C1sco12345 입니다. 아래 화면의 테이블 위에 있는 **Add** 버튼을 클릭하십시오.



5. 새 SGT 이름을 Research 로 지정하고 아이콘을 선택한 뒤 필요에 따라 주석을 추가하십시오. 새로운 그룹을 저장하기 위해 페이지 하단의 **Submit** 을 클릭하십시오.



6. ISE 창을 닫고 DNA Center 로 돌아가 **Policy dashboard** 로 갑니다.
7. Scalable Group 이 몇 개나 있습니까? 앞에서 확인했던 개수와 일치합니까?
8. **Registry** 클릭하고 사용 가능한 Scalable Groups 를 살펴보십시오. 거기에 새로 만든 Research 가 있습니까?

노트: 위 내용은 ISE 와 DNA Center 통합을 설명하기 위한 예입니다. 이 통합을 통해 사용자는 여러 화면에서 다양한 도구를 이용할 필요없이 신속하게 변경 작업을 수행 할 수 있도록 합니다. 향후에 ISE 와 DNA Center 간의 통합 기능은 향후에 보다 더 개선될 것입니다.

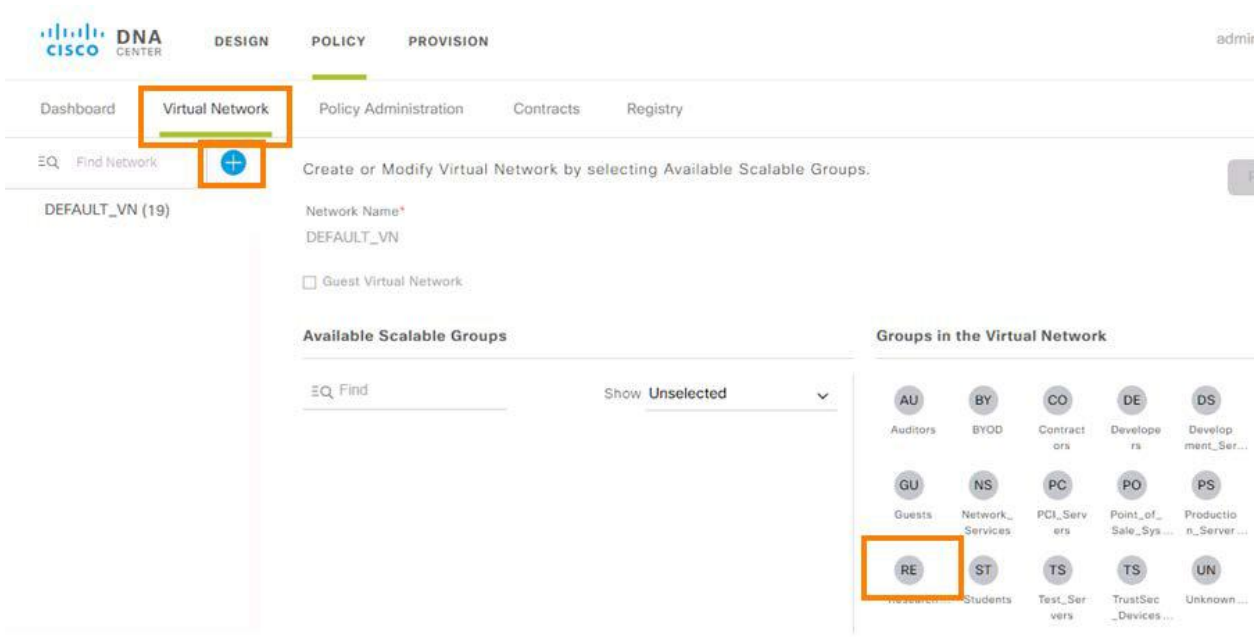
SD-Access 네트워크 세그멘테이션

이 부분은 대학교 환경에서의 SD-Access 구성을 시뮬레이션 해봅니다. 이를 통해 각 그룹 및 구성 요소들간의 SD-Access 가상화 및 세그멘테이션을 확인합니다.

1. **Policy > Virtual Network** 로 이동하십시오.

2. 맨 위에 가상 네트워크(**Virtual Networks**)를 추가로 생성할 수 있는 기능이 있습니다.

3. 기본 가상 네트워크(VN)에는 ISE-DNA Center 통합했기 때문에 ISE 에서 내려받은 시큐리티 그룹이 있습니다 (이전 단계에서 생성한 Research 그룹이 포함되어 있음).

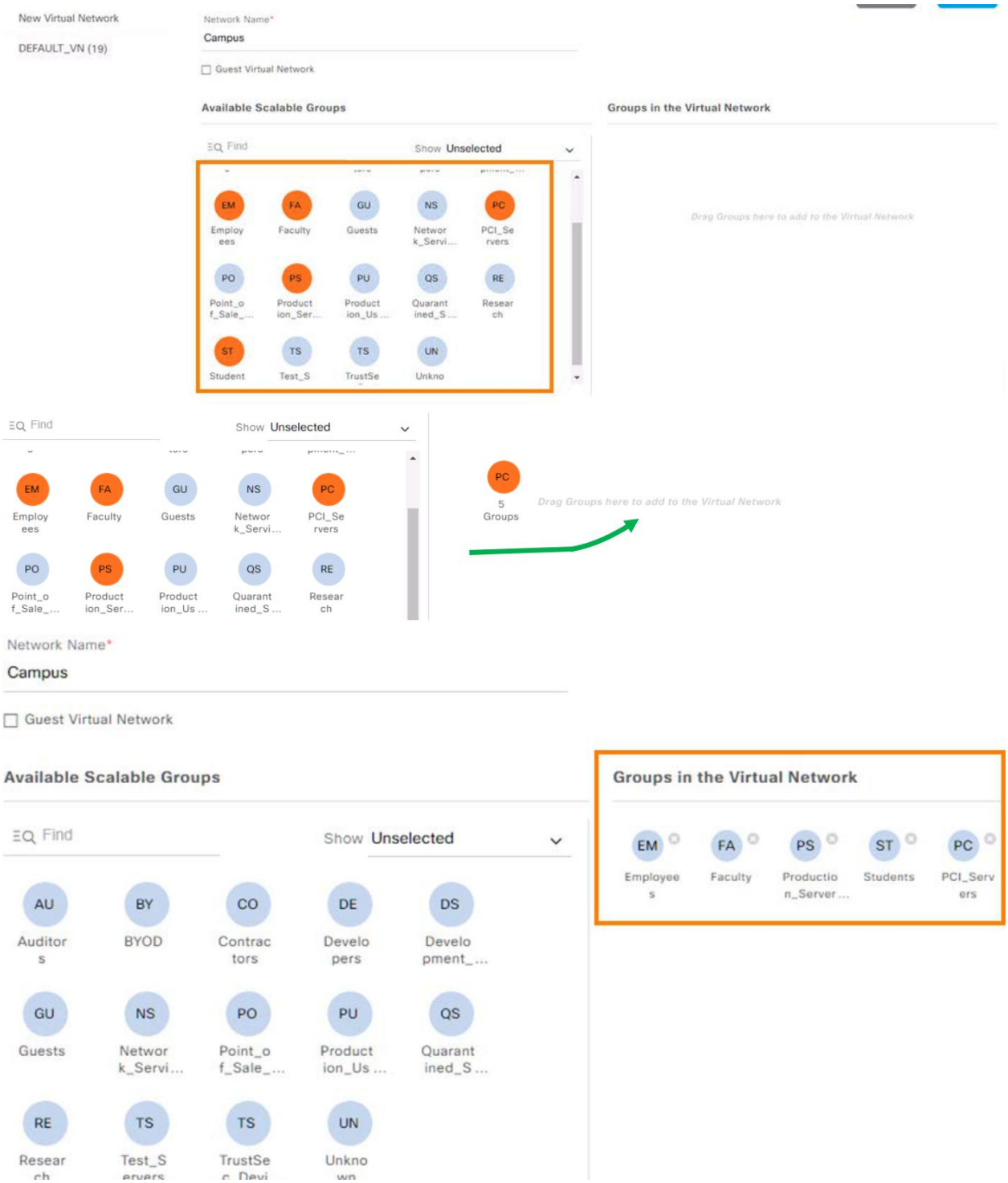


4. 새로운 **Virtual Network** 를 추가하기 위해 왼쪽에 보이는 ⊕ 클릭하십시오.

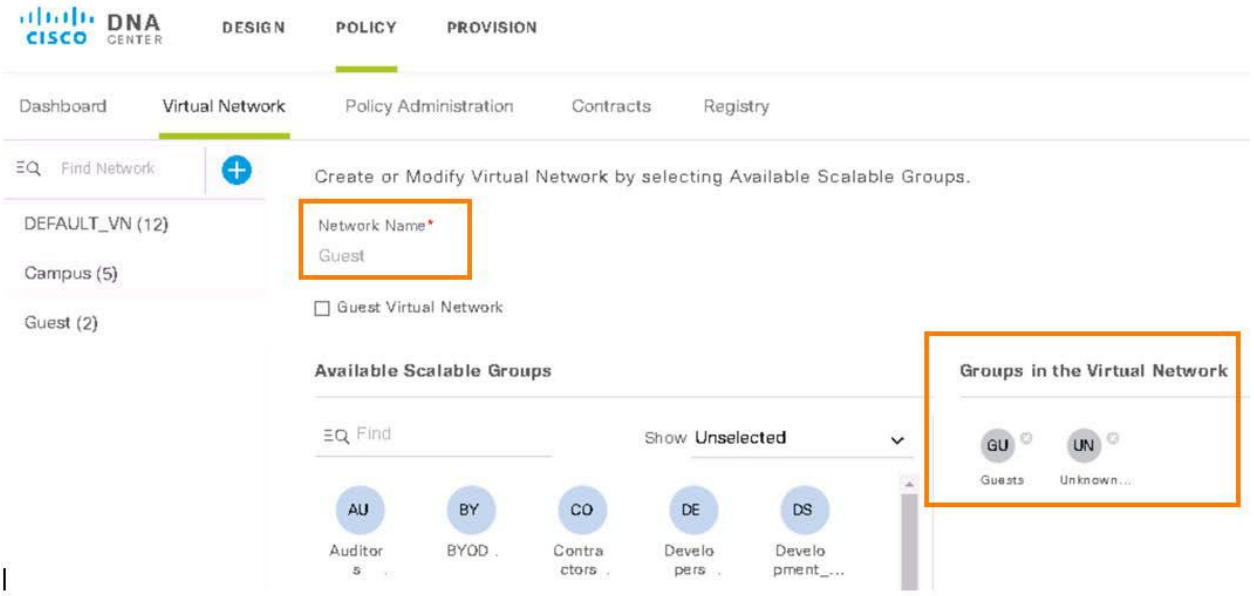
5. 그러면 새 가상 네트워크를 정의 할 수 있도록 창이 나타납니다. **Campus** 라는 이름으로 가상 네트워크 만드십시오

6. 저장하기 전 새로 만든 가상 네트워크에 그룹을 할당합니다. 이렇게 하면 가상 네트워크 내의 트래픽에 대하여 추가적인 세그먼트화가 가능합니다.

7. 다음 그룹을 선택하십시오**: Employees, Faculty, PCI_Servers, Production_Servers, Students**. 그런 다음, 선택한 그룹 중 하나를 클릭 한 채 가상 네트워크 박스로 드래그하여 놓습니다. 가상 네트워크에 5 개의 그룹이 모두 이동되었으면 변경 사항을 저장하십시오.



8. 위의 단계를 반복하여 Guest 라는 새 가상 네트워크를 만들고 Guests 및 Unknown 그룹을 게스트 네트워크로 이동합니다. 일단 완료되면 다음과 같이 표시됩니다.



9. 다음 단계로 이동하기 전에 **Save** 를 클릭하십시오.

SD- 액세스 정책 관리

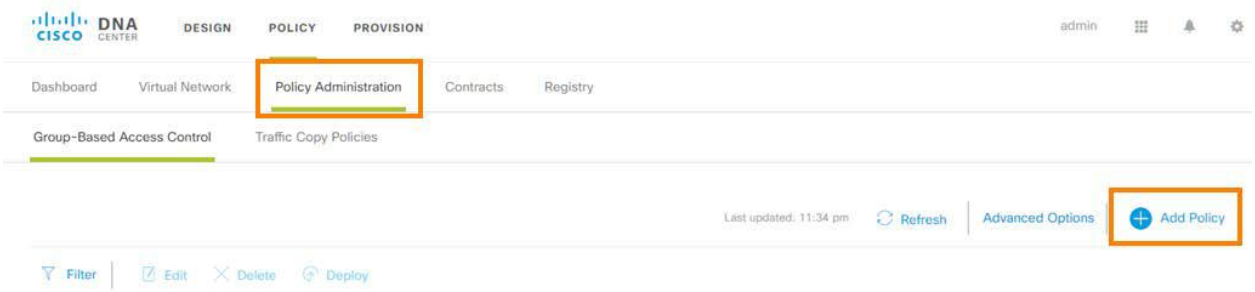
SD-Access 환경이 가상 네트워크로 분할되면 그 다음에는 보안 정책을 정의할 수 있습니다. DNA Center 는 가상 네트워크(VN) 내의 시큐리티 그룹간 트래픽을 거부하거나 명시적으로 허용할 수 있습니다.

다음 단계에서는, DNA Center 에서 몇 번의 클릭만으로 얼마나 손쉽게 보안 정책을 수립할 수 있는지를 보여줍니다.

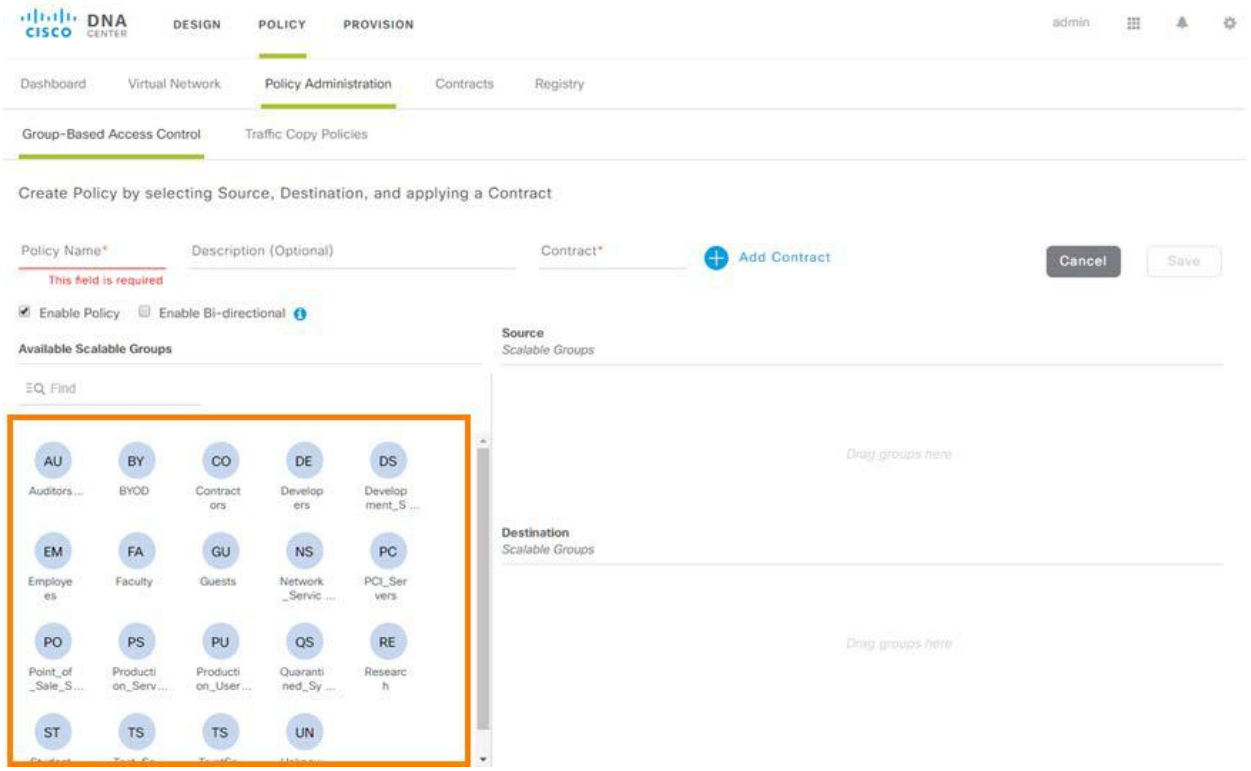
레이어 3 Contract 적용

1. **Policy > Virtual Networks** 페이지에서 **Policy Administration** (정책 관리)을 선택합니다.

2. 새 정책을 추가하기 위해 **Add Policy** 클릭하여 하십시오.

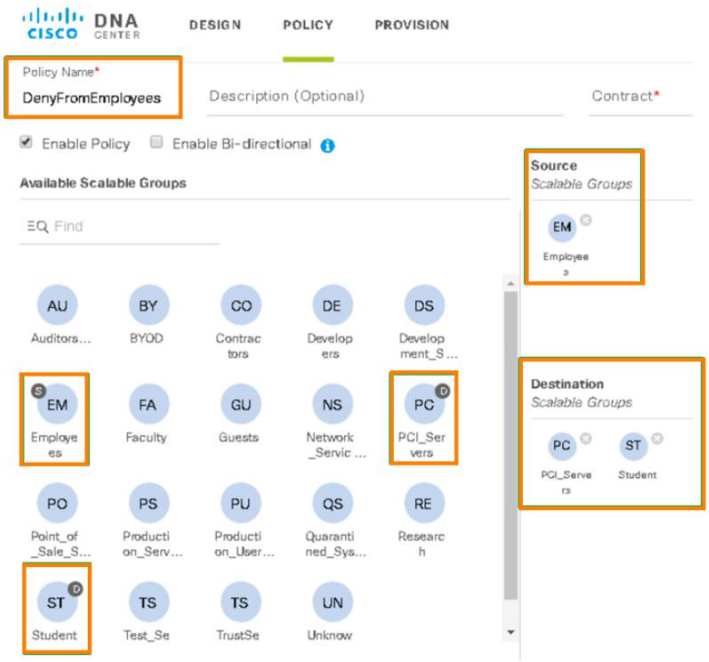


3. ISE 를 통해 DNA Center 에 추가된 Scalable Groups 이 표시됩니다. 여기에는 ISE 의 기본 Scalable 그룹 및 추가된 그룹이 몇 개 포함되어 있습니다.



4. 첫 번째 정책은 Employees 가 출발지이고 PCI_Servers 또는 Students 을 목적지로하는 트래픽을 거부하기 위한 **DenyFromEmployees** 정책을 만들겠습니다.

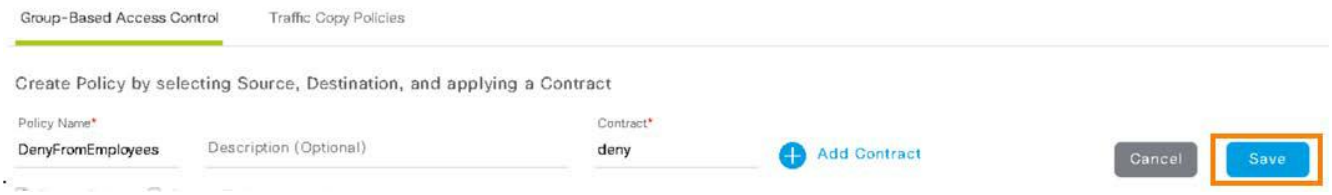
5. 먼저, 정책명을 **DenyFromEmployees** 로 입력합니다. 그런 다음 Employees 그룹을 선택하고 오른쪽의 Source 로 끌어다 놓습니다. 그리고 PCI_Servers 및 Students 를 오른쪽 Destination 박스로 끌어옵니다.



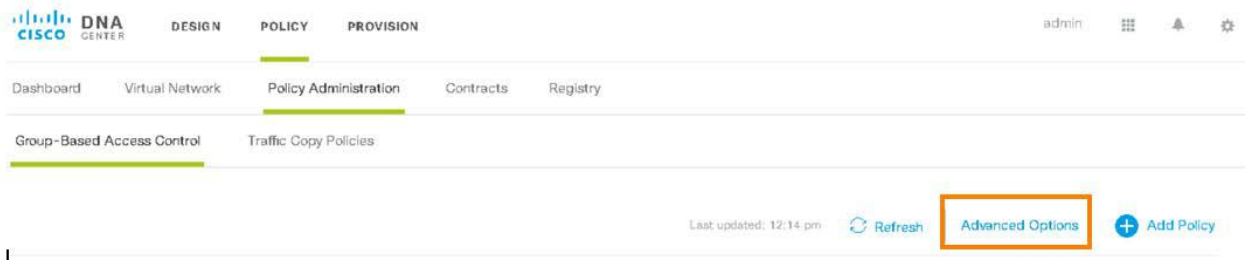
6. Scalable Groups 에 해당 **S** 및 **D** 가 강조 표시되어 할당된 정책을 나타냅니다.

7. Contract 추가를 위해 ⊕ 클릭합니다. Contract 필드에서 **deny** 를 선택하고 **OK** 를 클릭하십시오

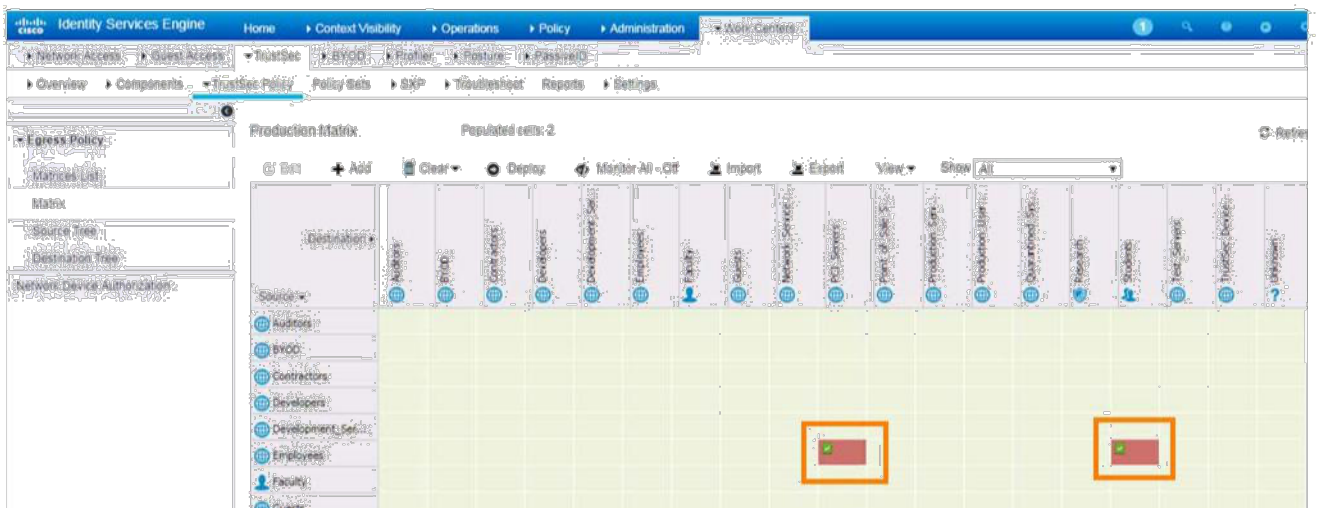
8. 정책이 올바른지 확인한 다음, 저장을 클릭하십시오.



9. 저장이 완료되면 Advanced Options 을 클릭하여 ISE 의 TrustSec Matrix 에 접근합니다. ISE TrustSec Matrix 의 브라우저 창이 열립니다. 로그인하라는 메시지가 표시되면 admin / C1sco12345 를 입력합니다.



노트: TrustSec Policy Matrix 구성은 몇 분 정도 소요됩니다. 잠시 기다려주십시오.



10. 최근 생성 된 **DenyFromEmployees** 정책이 빨간색으로 표시됩니다. 이것은 IP 거부 정책입니다.
11. DNA Center 에서 ISE 로 전송된 모든 정책을 보기 위해 다른 View 옵션을 선택할 수도 있습니다. **View > Condensed with SGACL Names** 로 접근합니다.
12. 나머지 레이어 3 정책 작성을 위해 2~9 단계를 반복하십시오.

테이블 7. Layer 3 정보

소스	Contract	목적지	Policy 명
PCI Servers	Deny	Production_Servers	DenyFromPCIServers
	Deny	Employees	
	Deny	Students	
Students	deny	Employees	DenyFromStudents
	Deny	PCI Servers	

노트: DNA Center 와 ISE 를 교차하며 작업을 수행하기 때문에 ISE 상의 TrustSec Matrix 의 확인/수정을 위해 DNA Center 를 닫지 않으셔도 됩니다.

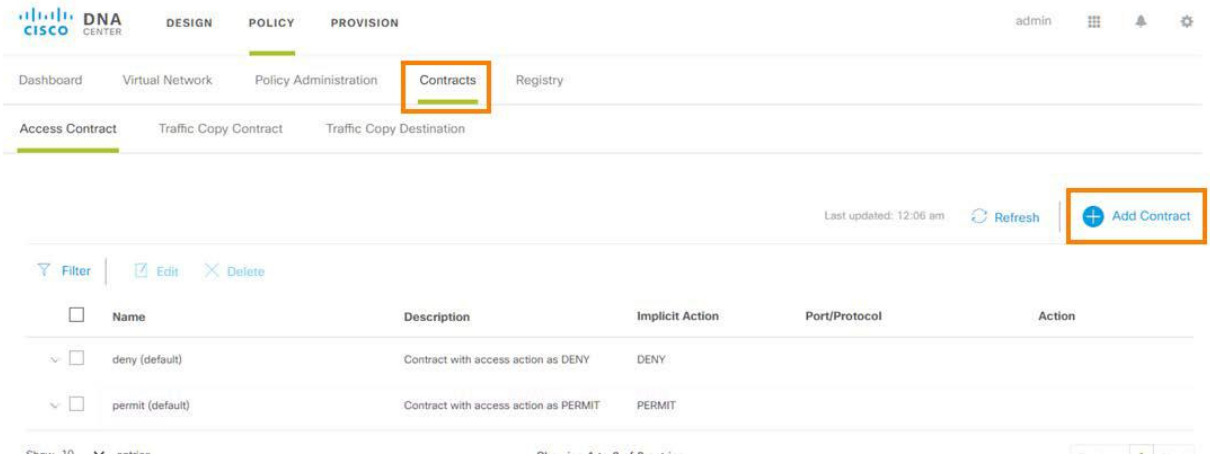
13. 마지막 정책을 추가한 후, ISE Matrix 로 돌아가서 View 를 새로 고칩니다. 다음과 같이 표시되어야 합니다

레이어 4 사용자 지정 Contract 적용하기

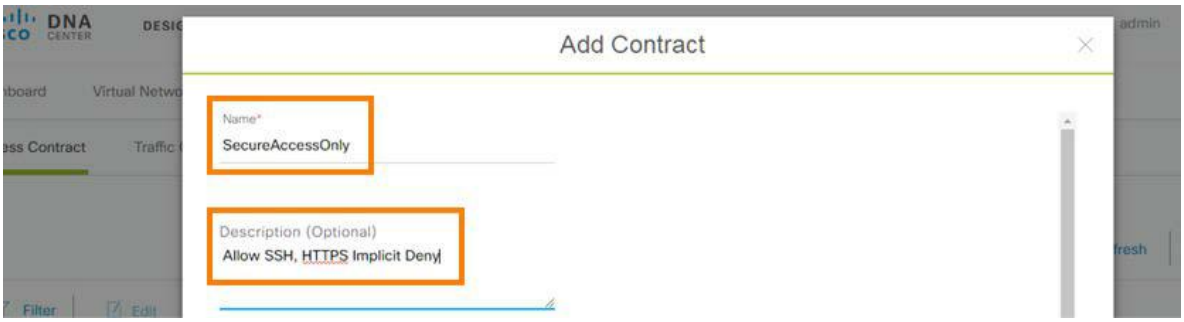
그룹간에 보다 세부적인 트래픽 제어를 수행하기 위해서는 커스텀 contract 이 필요합니다. 이 세션에서는 커스텀 contract 을 작성한 후 Faculty 그룹에 적용하는 방법을 안내합니다.

1. 커스텀 contract 을 작성하기 위해 **Policy app** 내의 **Contracts** 화면으로 이동합니다.

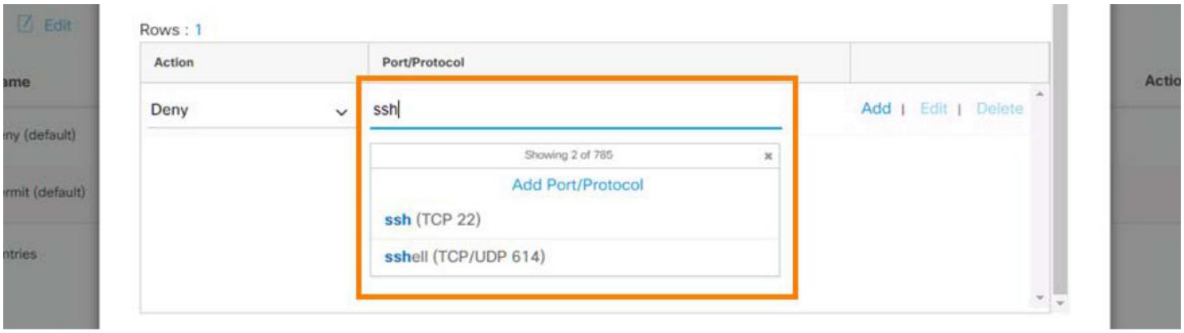
2. 여기서 기본적인 레이어 3 허가 및 거부 contract 을 볼 수 있습니다. 이 페이지의 오른쪽 위에 있는 **Add Contract** 을 클릭하여 커스텀 contract 대화 상자를 엽니다.

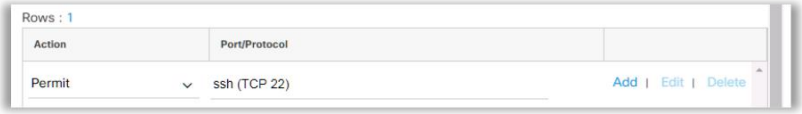


3. 대화 상자에서 **SecureAccessOnly** 으로 이름을 입력하고 주석에는 **Allow SSH, HTTPS Implicit Deny** 을 입력합니다.

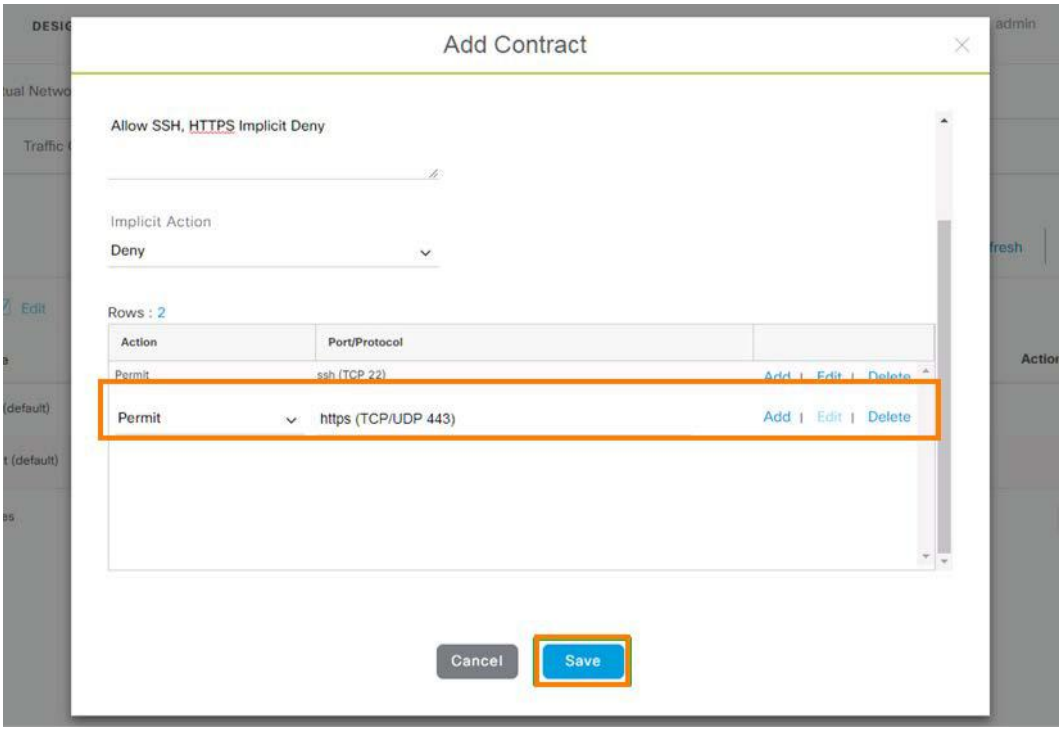


4. **Port/Protocol** 필드에 **ssh** 를 입력하고 SSH(TCP 포트 22)를 선택하십시오. **소문자 입력에 주의합니다.** 액션에서 **Permit** 을 선택하십시오. **Add** 를 클릭합니다.





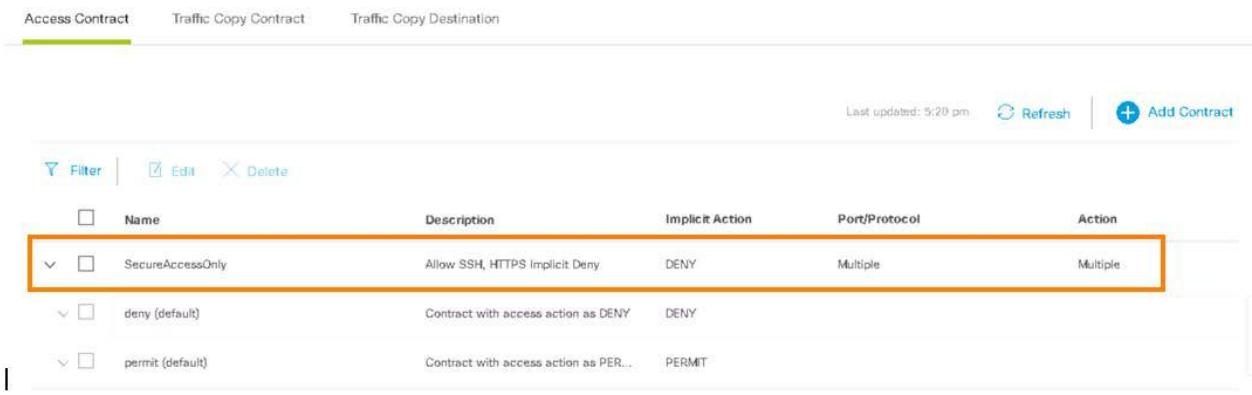
5. **https** 프로토콜을 선택하고 허용하기 위해 동일 작업을 수행합니다. **Add 는 클릭하지 마십시오. https** 는 소문자로 입력합니다.



6. **5 단계에서 Add 를 클릭한 경우에는 생성된 빈 항목은 삭제하십시오**. 그렇지 않으면 Contract 이 저장되지 않습니다.

7. 대화 상자 하단의 **Save** 을 클릭하십시오.

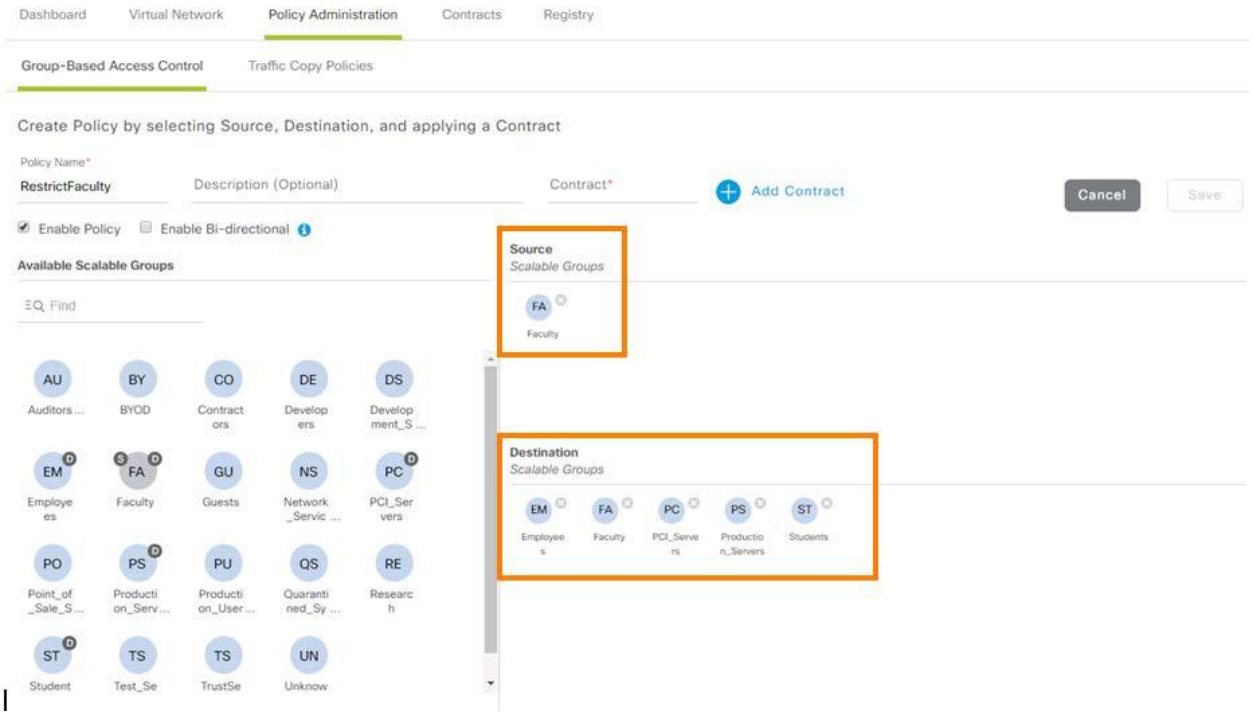
8. 저장하면 **SecureAccess Only** Contract 이 실제로 추가되었는지 확인할 수 있는 메인 Contract 페이지로 이동됩니다.



테이블 8. Secure Access 정보

출발지	Protocol	Contract	Contract 명	목적지	정책명
Faculty	ssh, https	allow		Employees	
Faculty	ssh, https	allow		Faculty	
Faculty	ssh, https	allow	SecureAccessOnly	PCI Servers	RestrictFaculty
Faculty	ssh, https	allow		Prod_Servers	
Faculty	ssh, https	allow		Students	

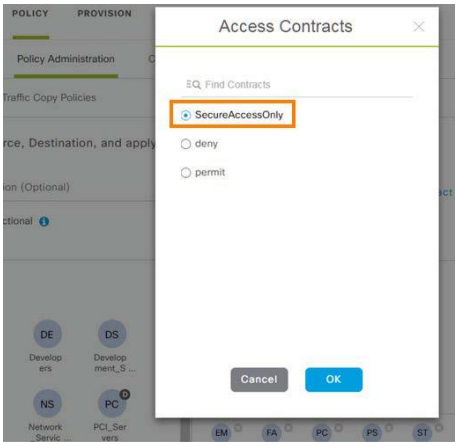
9. Policy Administration 페이지로 돌아가 **새 정책을 작성하십시오**. 정책명을 **RestrictFaculty** 로 지정하고 Faculty 그룹을 소스 박스로 드래그합니다.



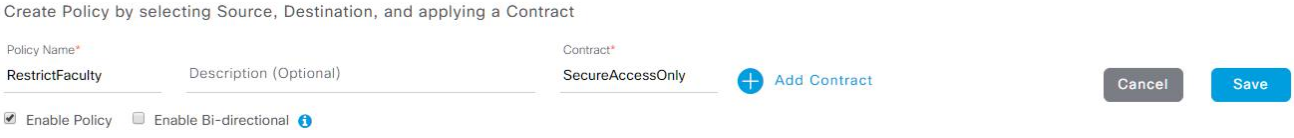
10. **Employees, Faculty, PCI_Servers, Students, Production_Servers** 를 선택하십시오. 다섯 개의 그룹을 Destination 으로 모두 끌어옵니다.

11. **Add Contract** 를 클릭합니다**.**

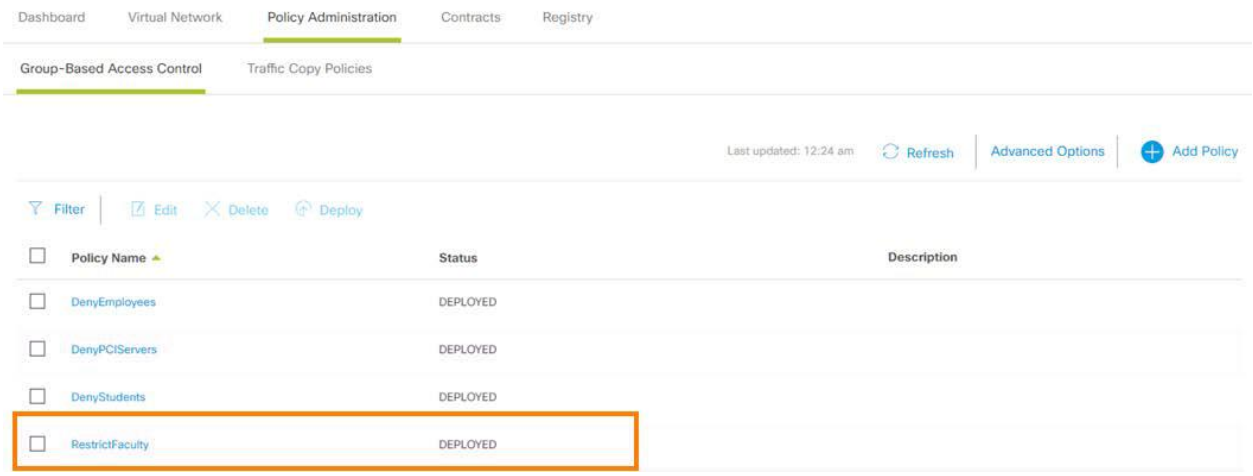
12. Contract 옵션에서 **SecureAccessOnly** 를 선택하고 **OK** 을 클릭하십시오.



13. 정책이 올바른지 확인하고 저장을 클릭하십시오.



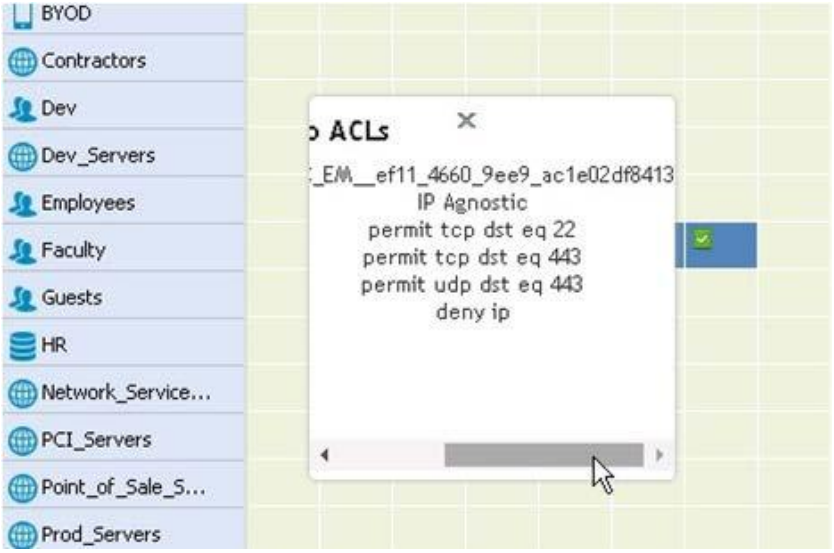
14. 완료되면 **Policy Administration** 페이지로 돌아가며 현재 저장된 정책이 정책 테이블에 있는지 확인할 수 있습니다.



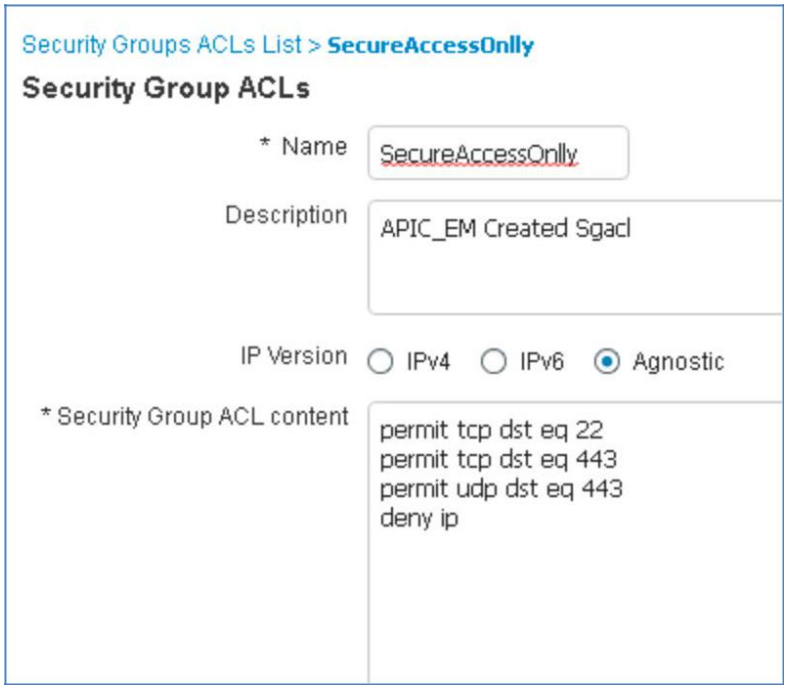
15. 다시 한번, **Advanced Options** 버튼을 사용하여 **ISE TrustSec Policy Matrix** 로 돌아갑니다. 로그인 해야하는 경우 admin / C1sco12345 을 입력합니다.

16. 레이어 4 ACE 가 적용된 새로운 파란색 셀이 생겨났는지 확인해야 합니다. 커스텀 contract 이름도 표시됩니다.

17. **파란색 셀에 마우스를 올려 놓고** Contract 이름 왼쪽의 아이콘 위로 마우스를 이동하면 DNA Center 를 통해 ISE 에 정의된 Layer-4 ACE 요약 정보를 표시하는 팝업 상자가 나타납니다.



18. 동일 정보를 확인하는 또 다른 방법은 ISE 의 **Work Centers > Trustsec > Compnents > Security Group ACLs** 로 이동한 다음 **SecureAccessOnly** 정책을 클릭하는 것입니다. 그러면 DNA Center 에서 적용한 시큐리티 그룹 ACL(Security Group ACL)이 표시됩니다.



19. 이 세션에서 설명한 워크 플로우를 이용하여 아래 테이블에 표시된 레이어 4 커스텀 contract 인 **SecureXfer** 를 만들고 **Policy** 로 적용합니다:

테이블 9. 정책

소스	프로토콜	Contract	Contract 명	목적지	정책명
Faculty	ssh, https	allow		Employees	
Faculty	ssh, https	allow		Faculty	
Faculty	ssh, https	allow	SecureAccessOnly	PCI Servers	RestrictFaculty
Faculty	ssh, https	allow		Prod_Servers	
Faculty	ssh, https	allow		Students	
PCI Servers	ssh, https, sftp	allow		PCI Servers	
PCI Servers	ssh, https, sftp	allow	SecureXfer	Faculty	RestrictPCIServers

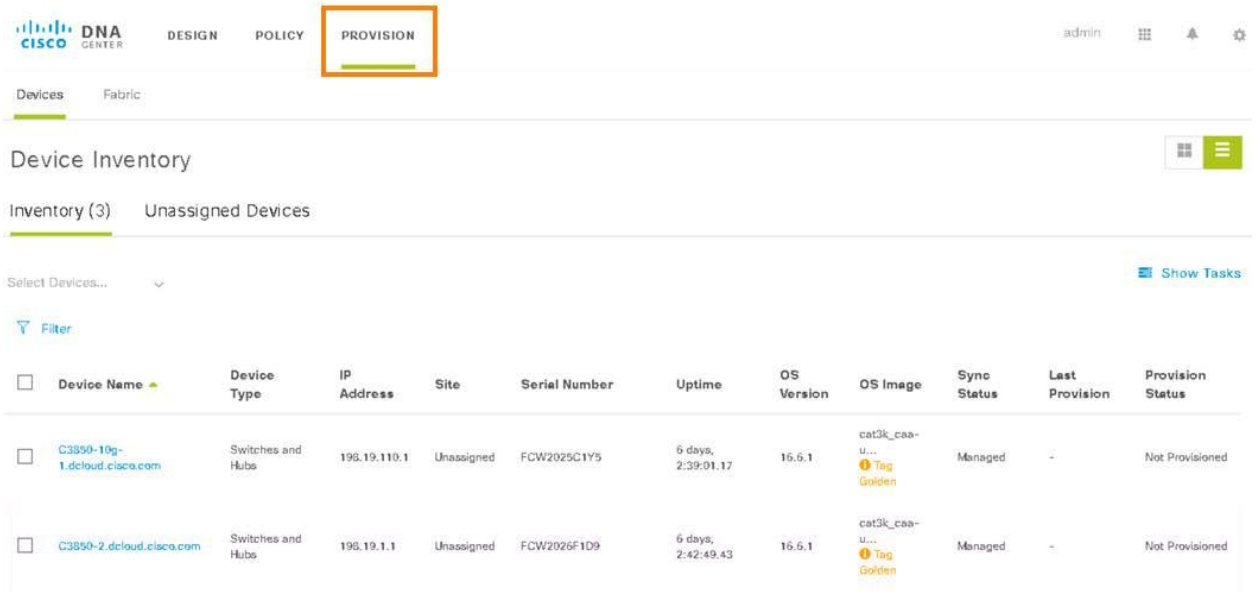
노트: 포트 / 프로토콜 목록 검색시에는 반드시 소문자를 사용하고 Contract 을 생성 할 때는 빈 작업은 삭제해야 합니다.

20. 완료되면 다음과 같이 **ISE TrustSec Policy Matrix** 가 표시됩니다:

시나리오 6. SD-Access Overlay 프로비저닝

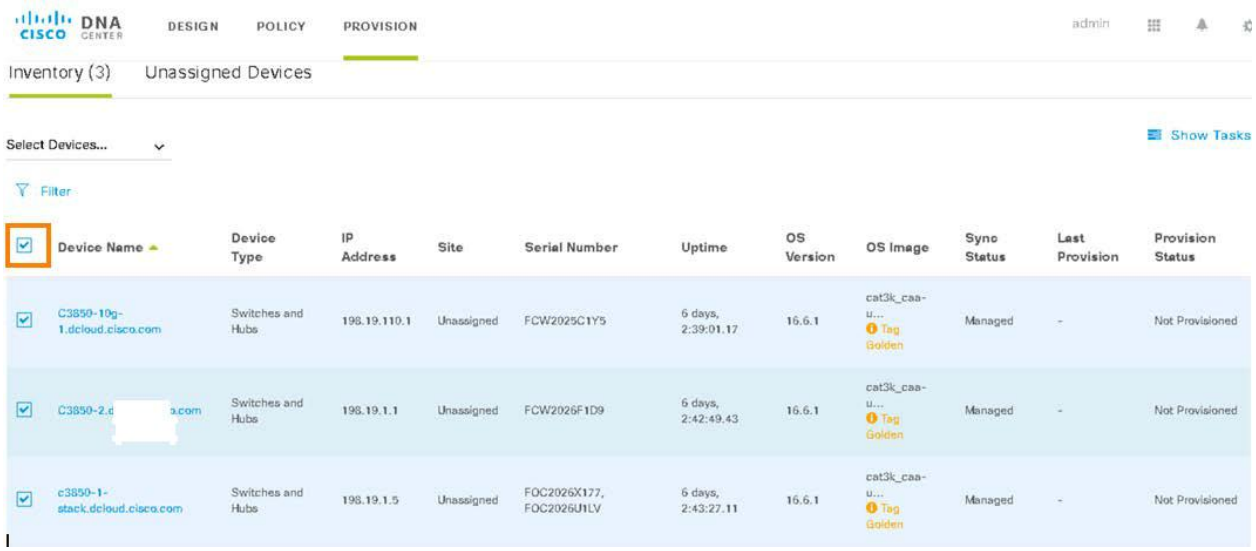
앞에서 정책을 구성했기 때문에 이제 오버레이 환경을 프로비저닝하고 호스트 온보딩을 시작할 수 있습니다.

1. 가장 위에 있는 메뉴에서 프로비저닝 App(Provision app)을 선택하십시오.



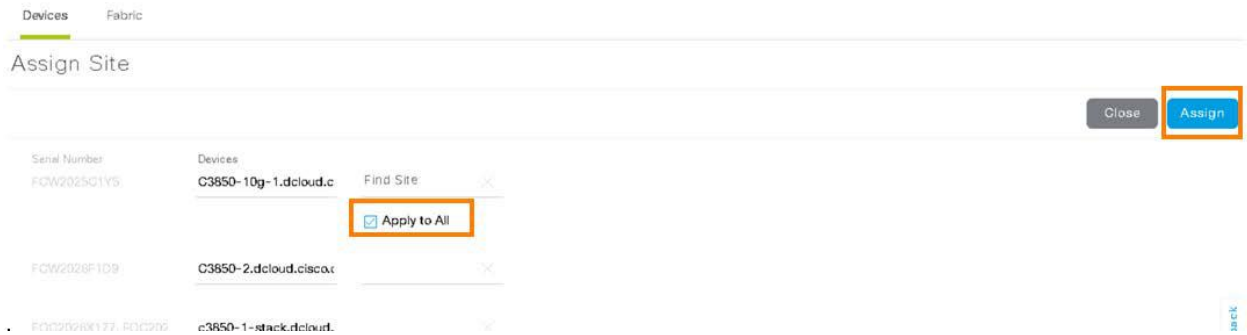
2. 프로비저닝 App 을 열면 디바이스 페이지로 이동합니다. 여기에서는 장치를 선택하고 디자인 단계에서 만든 물리적 사이트에 연결시켜 프로비저닝 프로세스를 시작할 수 있습니다.

3. **Device Name** 옆의 박스를 클릭하여 모든 장치를 선택하십시오.

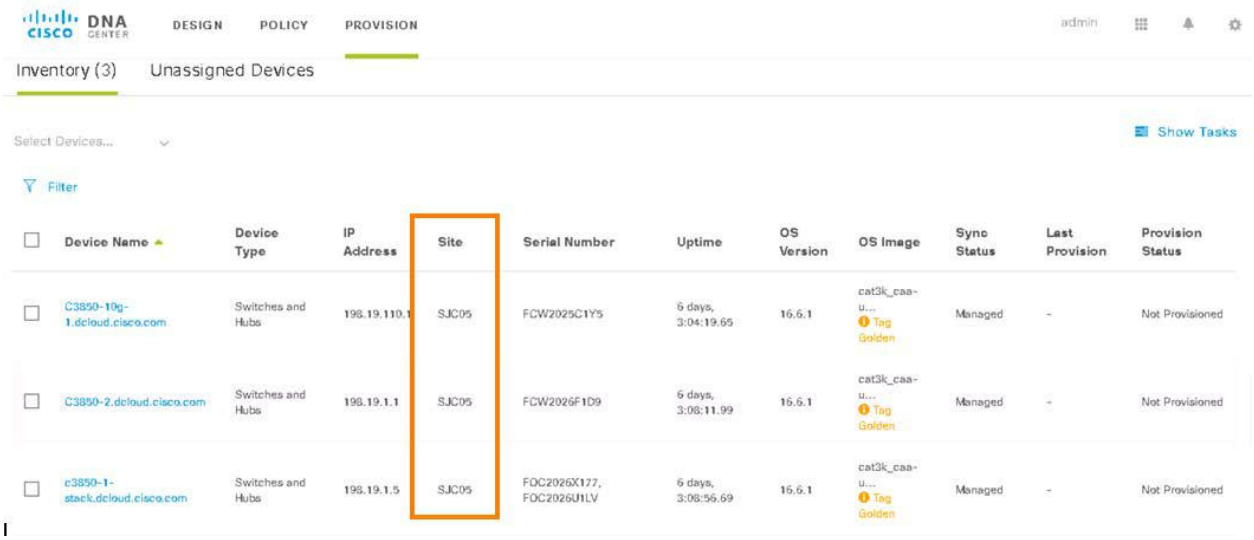


4. 장치가 모두 선택한 뒤 Selected Devices 를 클릭하여 **Add/Remove Site** 를 선택하십시오.

5. 동일 사이트에 할당하기 위해 Apply to All 에 체크하고 사이트명 입력란에 **SJC05** 를 입력하십시오. 입력 시 디자인 단계에서 생성한 사이트명이 자동 완성됩니다. 사이트가 선택되면 **Assign** 을 클릭하십시오.

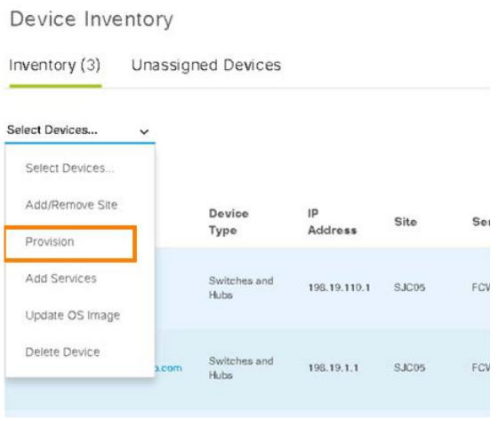


6. 장치를 **SJC05** 사이트에 추가하면 인벤토리 페이지가 나타나며 DNA Center 의 변경 사항에 대한 피드백 정보가 표시됩니다. Site 는 업데이트 되었지만 장치가 아직 프로비저닝 되지는 않았습니다.

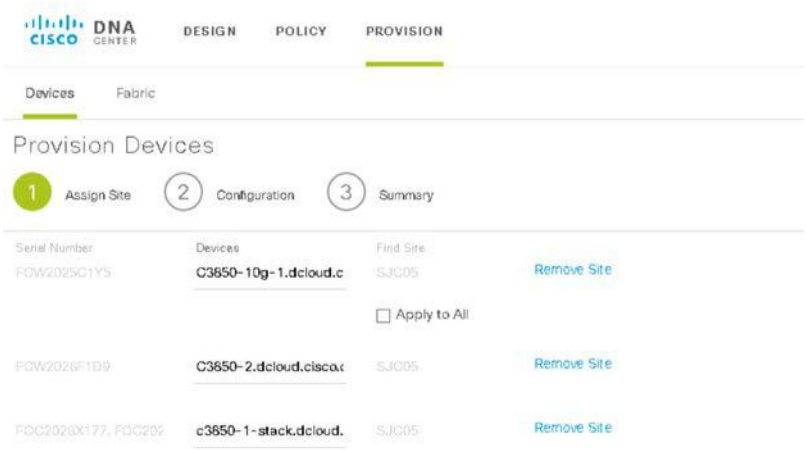


7. 사이트에 추가되면 장치를 다시 모두 선택한 다음 Selected Devices 를 클릭하여 **Provision** 을 선택하십시오

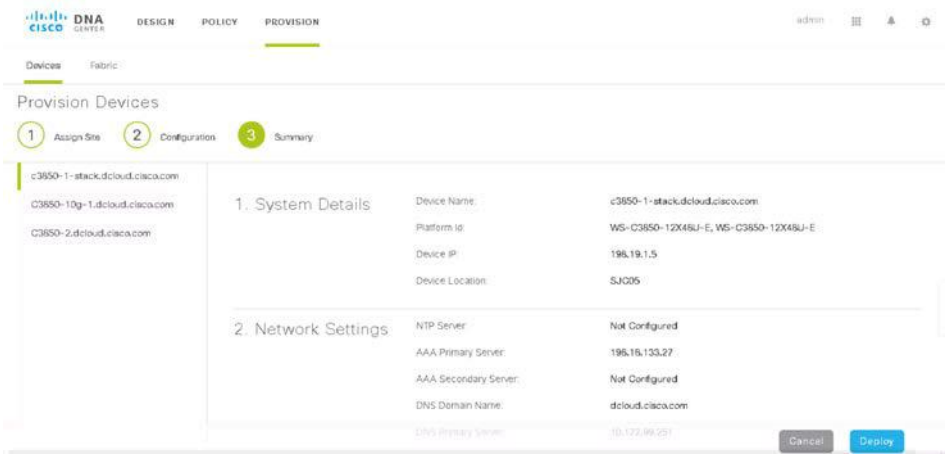
노트: 동일 유형의 장치만 (예 : Cat3K 는 스위치 및 허브 종류로 분류됨) 동시에 프로비저닝할 수 있습니다.



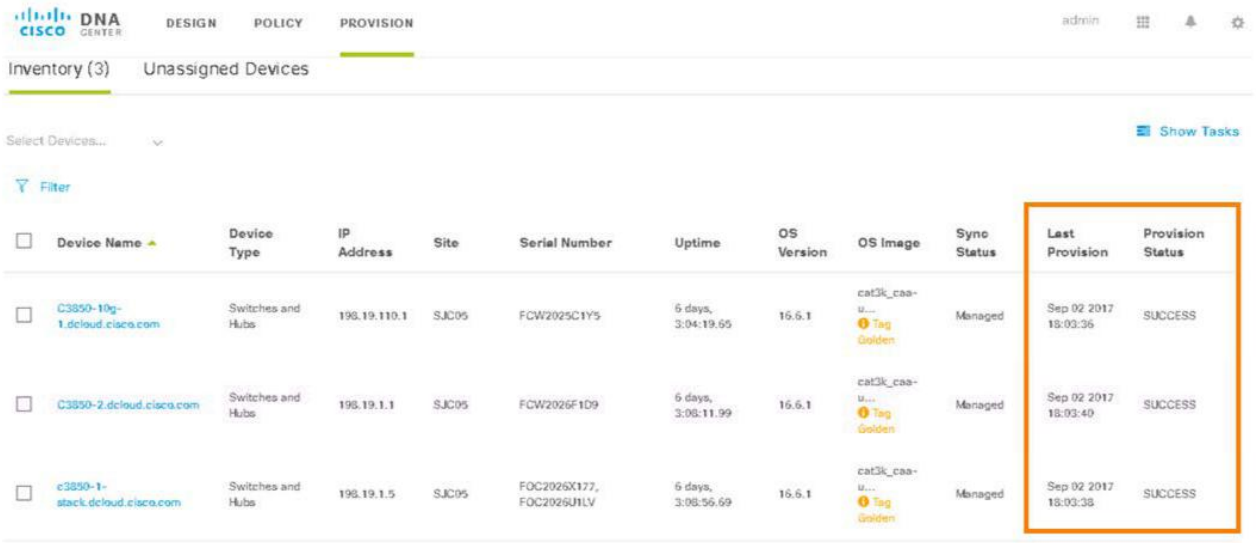
8. 모든 장치가 SJC05 사이트로 할당되었는지 확인한 후 **Next** 를 클릭합니다.



9. Configuration 단계는 현시점에서 어떤 작업도 하지 않기 때문에 건너 뜁니다.
10. **Summary** 페이지에서, DNA Center 가 장치에 어떤 정보를 내보내는지 확인한 뒤에 **Deploy** 를 클릭하십시오.



11. 완료 후, DNA Center 가 디바이스 페이지로 리다이렉트됩니다. **Inventory** 화면에 장치가 구성되었다고 표시됩니다



12. 장치가 프로비저닝되었으므로, **MTPuTTY** 를 사용하여 스위치에 접속해 DNA Center 에서 적용한 구성 내용을 확인합니다.

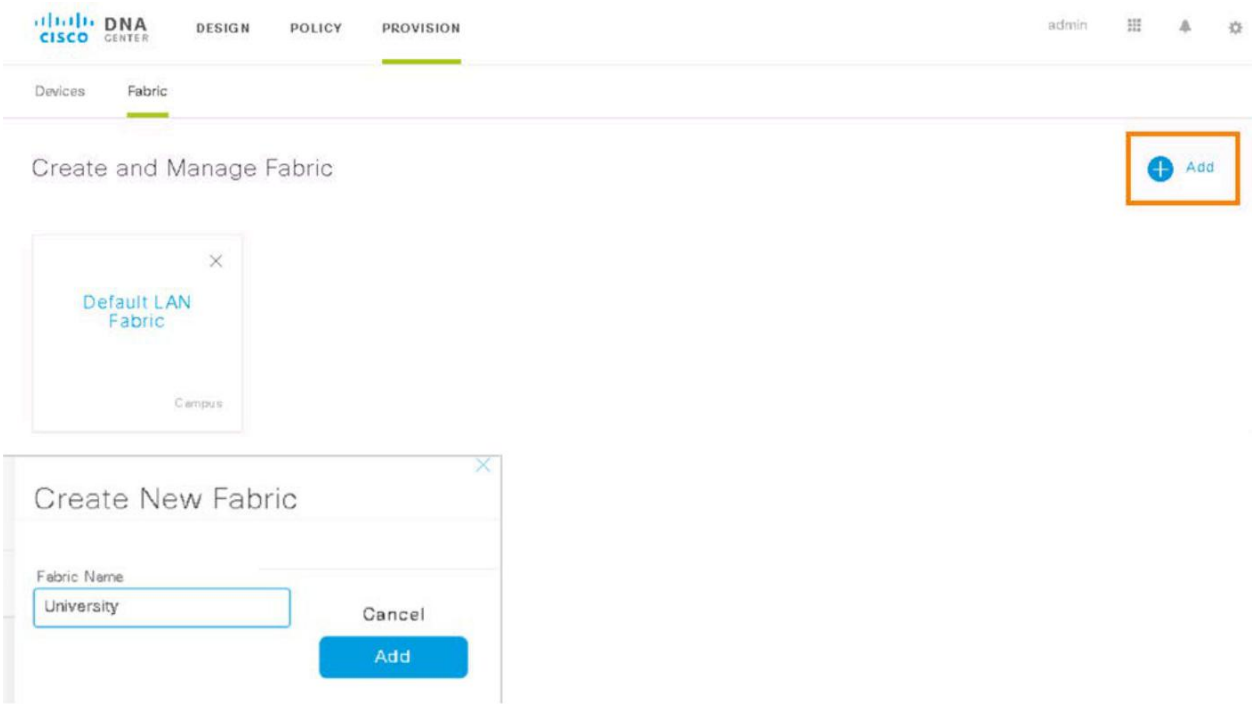
```
C3850-2#show run | sec aaa
aaa new-model
aaa group server radius dnac-radius-group
 server name dnac-radius_198.18.133.27 ip
 radius source-interface Loopback0
aaa authentication login default local aaa
authentication enable default enable
aaa authentication dot1x default group dnac-radius-group
aaa authorization exec default local
aaa authorization network default group dnac-radius-group
aaa authorization network dnac-cts-list group dnac-radius-group
aaa accounting dot1x default start-stop group dnac-radius-group
aaa login server radius dynamic-author
 client 198.18.133.27 server-key C1sco12345

aaa session-id common

C3850-2#show run | sec radius
aaa group server radius dnac-radius-group
 server name dnac-radius_198.18.133.27 ip
 radius source-interface Loopback0
aaa server radius dynamic-author
 client 198.18.133.27 server-key C1sco12345
ip radius source-interface Loopback0
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 2 tries 1
radius server dnac-radius_172.26.204.121
 address ipv4 198.18.133.27 auth-port 1812 acct-port 1813
 pac key C1sco12345


C3850-2#show run | sec cts
aaa authorization network dnac-cts-list group dnac-radius-group

cts authorization list dnac-cts-list

C3850-2#show cts pac
AID: E931DE3291C8F09570B99C1A7545D9F8
PAC-Info:
 PAC-type = Cisco Trustsec
 AID: E931DE3291C8F09570B99C1A7545D9F8
 I-ID: C3850-2.cisco.com
 A-ID-Info: Identity Services Engine
 Credential Lifetime: 16:00:48 UTC Fri Sep 23 2017
```

13. 오류가 있으면 상태에 오류가 표시됩니다. 만약 구성에 이슈가 있으면 DNA Center 는 변경 사항을 자동으로 롤백시킵니다. 정보 아이콘 위에 마우스를 가져다 대면 오류 내용을 볼 수 있습니다 (지금은 존재하지 않아야 함).

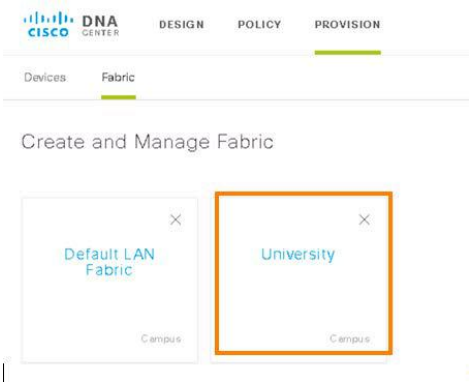
패브릭 생성 및 관리

이제 DNA Center 는 장치가 어느 사이트에 있는지 알고 있기 때문에 패브릭 프로비저닝을 시작할 수 있습니다.

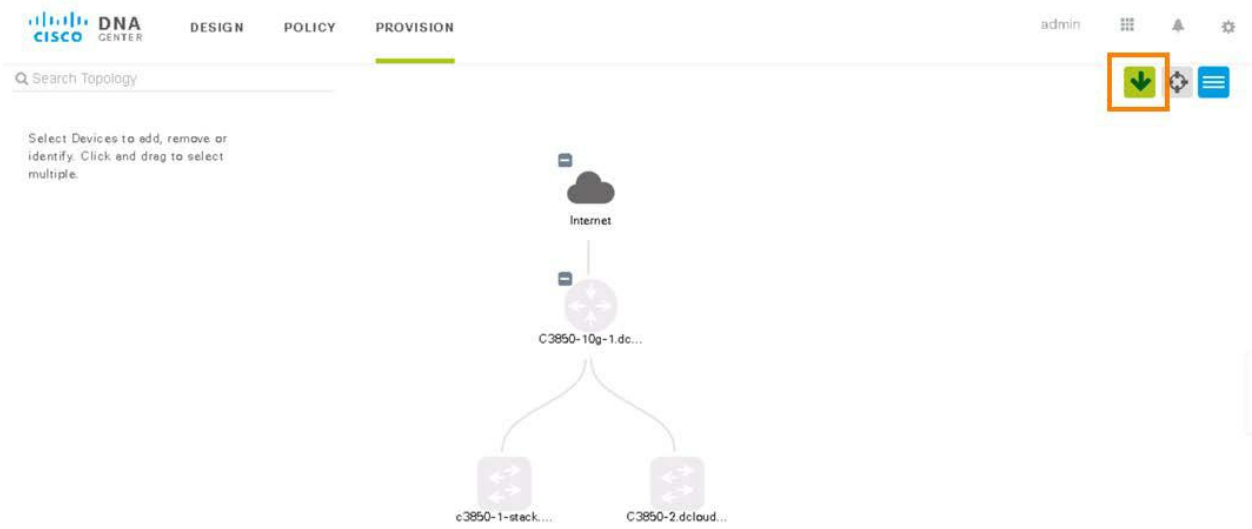
1. 메뉴를 사용하여 **Fabric** 을 선택하십시오. 잠시 후 SD-Access 패브릭을 만들고 관리할 수 있는 새로운 페이지로 이동합니다 .
2. **Add create a new Fabric** 클릭하고 이름을 **University** 로 지정하십시오.



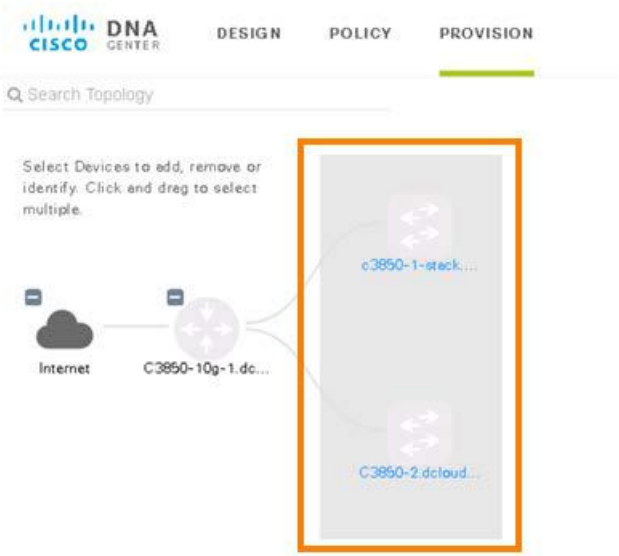
3. 생성이 완료되면 **University** 패브릭 박스를 클릭하여 프로비저닝을 시작하십시오



4. University 패브릭으로 들어가면 이 Lab 환경의 토폴로지가 수직형 레이아웃으로 표시됩니다. 레이아웃을 수평으로 바꾸려면 **아래쪽 화살표가 있는 녹색 박스를 클릭하십시오**.

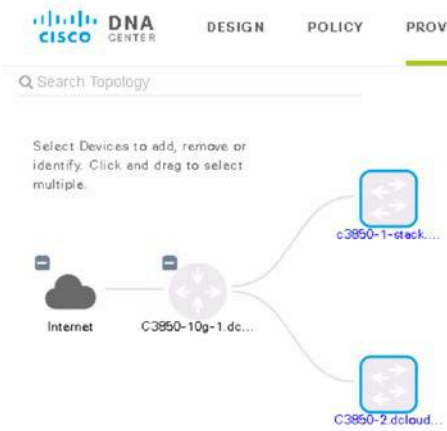


5. 마우스 왼쪽 버튼을 누른 상태에서 드래그하여 **C3850-1-stack** 와 **C3850-2 access switches** 를 묶으면 강조 표시가 됩니다.

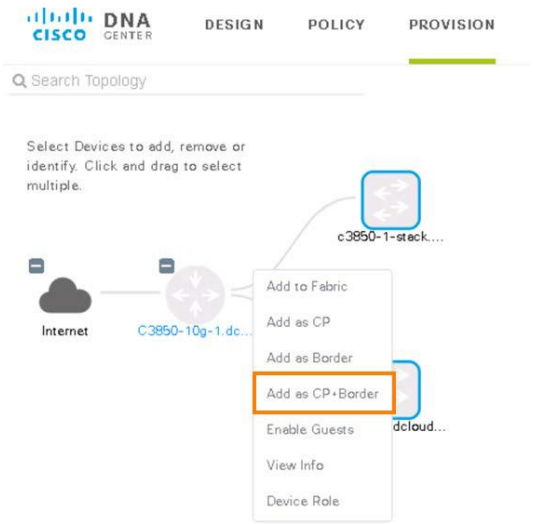


6. 마우스 왼쪽 버튼을 놓으면 패브릭에 추가하는 기능이 표시됩니다. 기본적으로 Add to Fabric 를 선택하여 추가된 모든 장치들은 패브릭 Edge 노드로(Edge nodes) 간주됩니다.

7. 일단 패브릭에 추가되면 장치에 파란색 윤곽선이 표시됩니다.



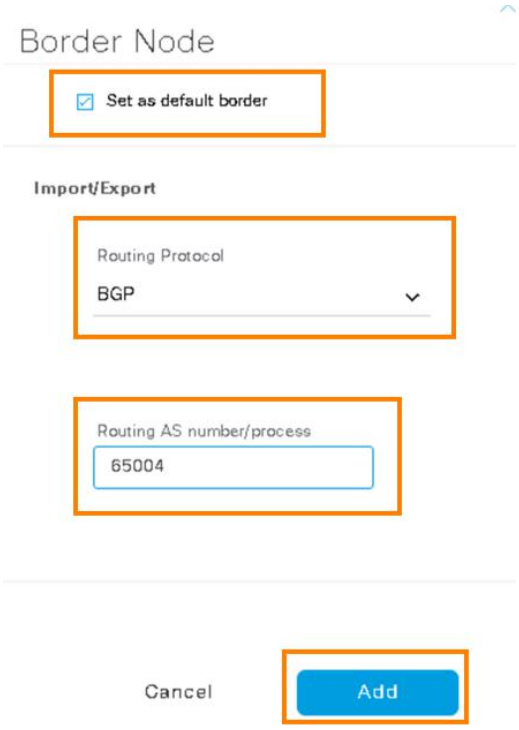
8. 경계(Border) 및 컨트롤 플레인(Control Plane) 노드를 명시적으로 정의해야 합니다. **C3850-10g-1** 을 클릭하고 **Add as CP+Border** 를 선택하십시오.



9. 그러면, Border 노드를 설정할 수 있는 대화 상자가 열리며 여기에서는 해당 장비를 **Default Border** 로 설정 유무, 라우팅 프로토콜 선택 및 BGP 번호를 입력할 수 있는 대화 상자가 열립니다.

10. 다음 값과 입력하십시오.

    - Set as default border 설정에 체크
    - 프로토콜을 BGP 로 남겨 두십시오
    - Routing AS number 에 **65004** 입력
    - 다음 단계로 가려면 Add 를 클릭.



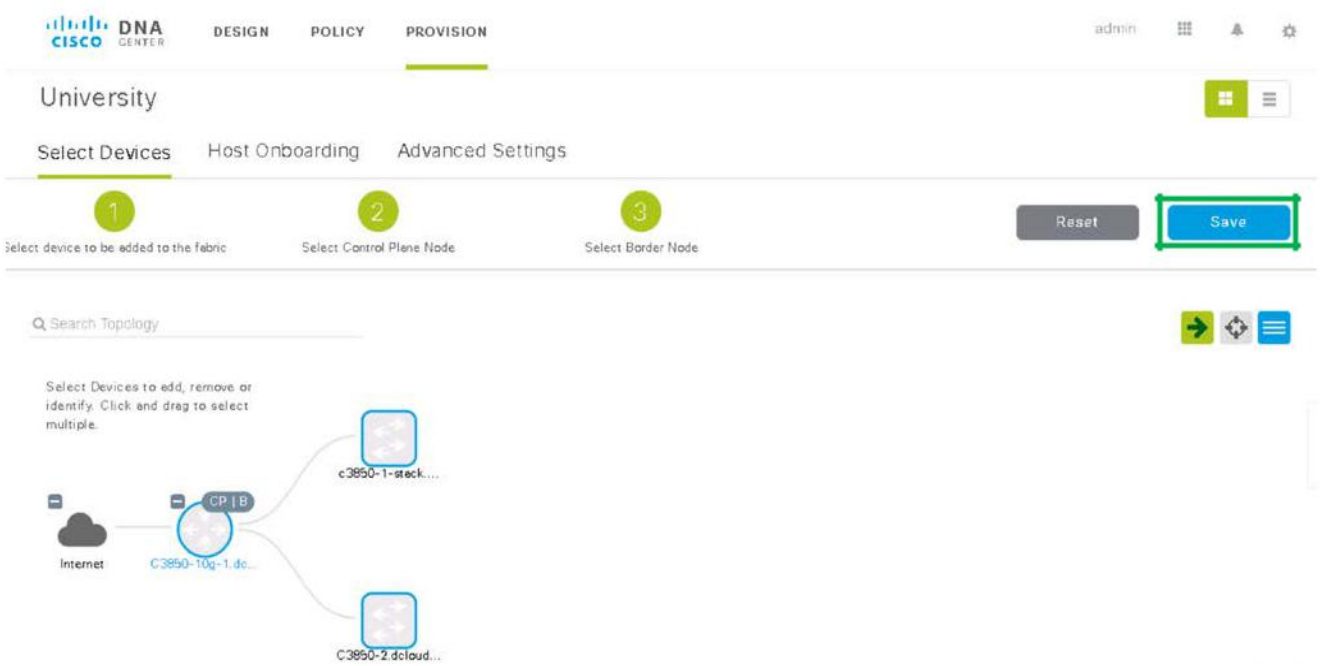
11. 스위치에 접속하여 다음 명령을 실행한 뒤 출력을 확인합니다:

```
show run vrf

show run | sec lisp
```

앞서 수행한 내용의 관련 Configuration 양은 매우 적습니다. (있는 경우).

12. DNA Center 화면으로 돌아가 **Save** 를 클릭하십시오.

노트: 저장에는 약 1 ~ 2 분 소요되므로 잠시 기다려주십시오.



노트: 장치가 패브릭에 프로비저닝된 후에는 노드가 파란색 테두리로 표시됩니다.

13. Devices 페이지의 오른쪽 위에 있는 Save 버튼을 클릭하면 가상 네트워크(VN) 및 LISP (호스트 데이터베이스) 구성을 Border 및 Edge 노드로 내려보내게 됩니다. 새롭게 추가된 Configuration 구성을 보려면 각 노드에 로그인하십시오. 다음과 같은 항목이 새롭게 표시됩니다.

```
Border node:
C3850-10g-1#show run | section
 lisp router lisp
 locator-table default
 locator-set rloc_2490ab0d-49ff-4c13-9da1-eae229ff3c9c
  IPv4-interface Loopback0 priority 10 weight 10 exit-
  locator-set
 !
 service ipv4
  encapsulation vxlan
  map-cache-limit 25000
  database-mapping limit dynamic
  5000 itr map-resolver 198.19.110.1
  etr map-server 198.19.110.1 key uci
  etr map-server 198.19.110.1 proxy-reply
  etr
  sgt
  proxy-etr
  proxy-itr 198.19.110.1
  map-server
  map-resolver
  exit-service-ipv4
 !
```

Overlay Border Configuration

Overlay Control Plane Configuration

```
  map-cache-limit 25000
  database-mapping limit dynamic 5000
  map-server
  map-resolver
  exit-service-ethernet
 !
 instance-id 4097
  remote-rloc-probe on-route-change
  service ipv4
   eid-table vrf DEFAULT_VN route-
   export site-registrations
   distance site-registrations 250
   map-cache site-registration
   exit-service-ipv4
  !
  exit-instance-id
 !
 instance-id 4098
  remote-rloc-probe on-route-change
  service ipv4
   eid-table vrf Campus route-
   export site-registrations
   distance site-registrations 250
   map-cache site-registration
   exit-service-ipv4
  !
  exit-instance-id
 !
 instance-id 4099
  remote-rloc-probe on-route-change
  service ipv4
   eid-table vrf Guest route-
   export site-registrations
   distance site-registrations 250
   map-cache site-registration
   exit-service-ipv4
  !
  exit-instance-id
 !
 site site_uci
  description map-server configured from apic-em
  authentication-key uci
  eid-record instance-id 4097 0.0.0.0/0 accept-more-specifics
  eid-record instance-id 4098 0.0.0.0/0 accept-more-specifics
  eid-record instance-id 4099 0.0.0.0/0 accept-more-specifics
  exit-site
```

Default Virtual Network

Campus Virtual Network

Guest Virtual Network

Edge node1 (C3850-2):

```
C3850-2#show run | section lisp
router lisp
 locator-table default
 locator-set rloc_c17a073e-f7f4-4329-8985-ee73e03e4997
  IPv4-interface Loopback0 priority 10 weight 10
  exit-locator-set
 !
```

```
locator default-set rloc_c17a073e-f7f4-4329-8985-ee73e03e4997
service ipv4
 encapsulation vxlan
 map-cache-limit 25000
 database-mapping limit dynamic 5000
 itr map-resolver 198.19.110.1
 itr
 etr map-server 198.19.110.1 key uci
 etr map-server 198.19.110.1 proxy-reply
 etr
 sgt
 use-petr 198.19.110.1
 exit-service-ipv4
!
service ethernet
 map-cache-limit 25000
 database-mapping limit dynamic 5000
 itr map-resolver 198.19.110.1
 itr
 etr map-server 198.19.110.1 key uci
 etr map-server 198.19.110.1 proxy-reply
 etr
 exit-service-ethernet
!
instance-id 4097
 remote-rloc-probe on-route-change
 service ipv4
  eid-table vrf DEFAULT_VN
  exit-service-ipv4
 !
 exit-instance-id
!
instance-id 4098
 remote-rloc-probe on-route-change
 service ipv4
  eid-table vrf Campus
  exit-service-ipv4
 !
 exit-instance-id
!
instance-id 4099
 remote-rloc-probe on-route-change
 service ipv4
  eid-table vrf Guest
  exit-service-ipv4
 !
 exit-instance-id
!
encapsulation vxlan
ipv4 locator reachability exclude-default
exit-router-lisp
```

Path to Default Border

Default Virtual Network

Campus Virtual Network

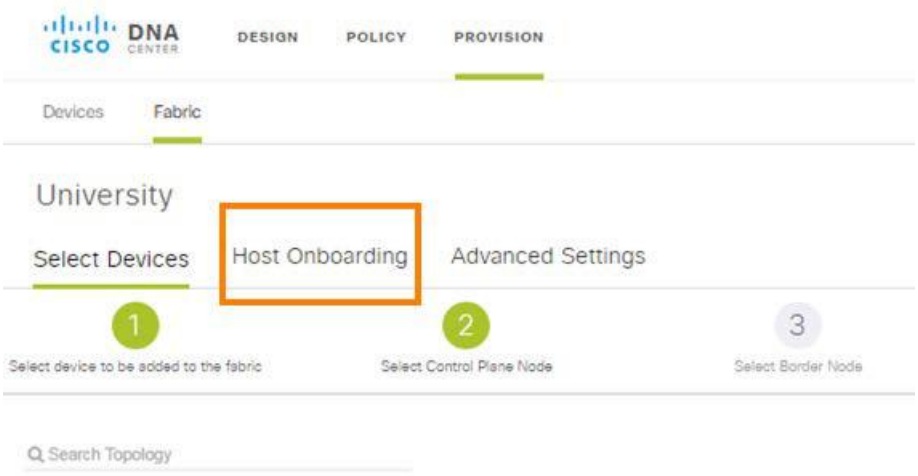
Guest Virtual Network

시나리오. 7 SD-Access 엔드 호스트 프로비저닝

Overlay 가 프로비저닝 완료되면 호스트들이 패브릭 내부에서 통신할 수 있도록 IP 어드레스 Pool 이 추가되어야 합니다. SD-Access 환경에서 IP Pool 이 구성되면 DNA Center 는 즉시 각 Edge 노드에 연결하여 호스트들이 통신 할 수 있도록 SVI(Switch Virtual Interface)인터페이스를 구성합니다.
그리고, 애니캐스트 게이트웨이(Anycast gateway)는 모든 에지 노드에 적용됩니다. 호스트가 추가 프로비저닝 없이 다른 에지 노드로 쉽게 로밍될 수 있도록 해주는 SD-Access 의 필수 요소입니다.

스텝:

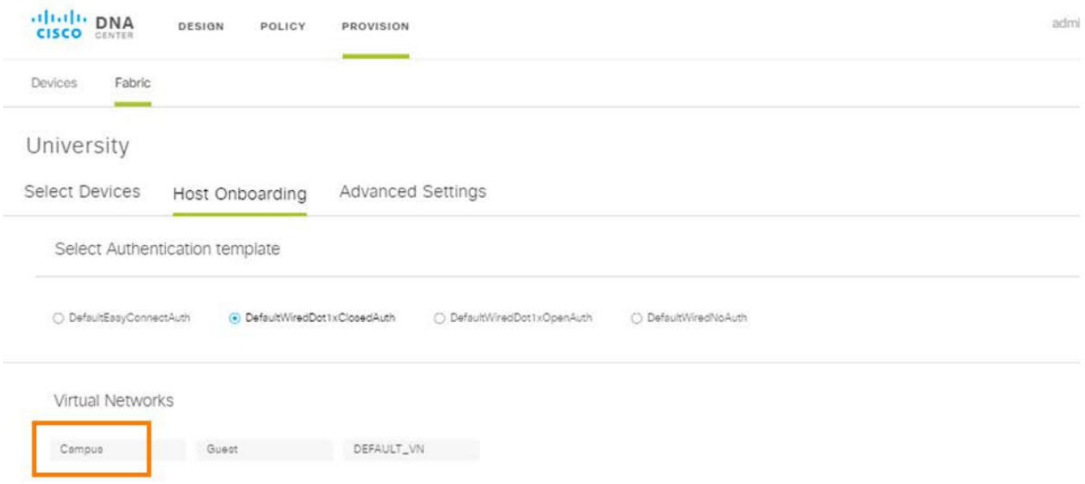
1. 화면의 상단에 있는 **Host Onboarding** 을 클릭하여 호스트 장치들에 대한 IP Pool 작성을 시작합니다.

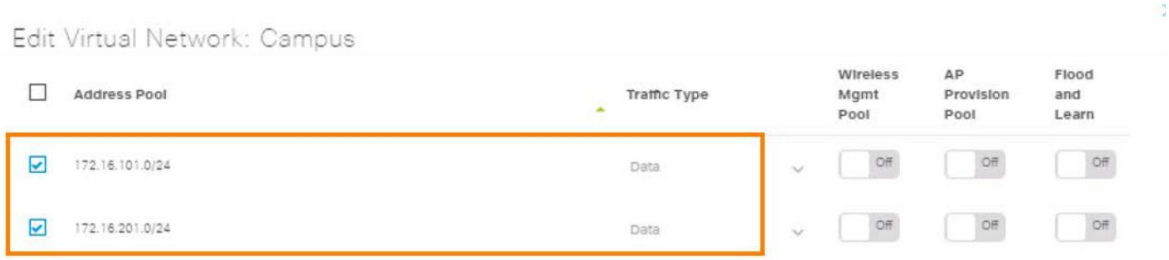


2. **DefaultWiredDot1xClosedAuth** 선택하고 **Save** 를 클릭하십시오.

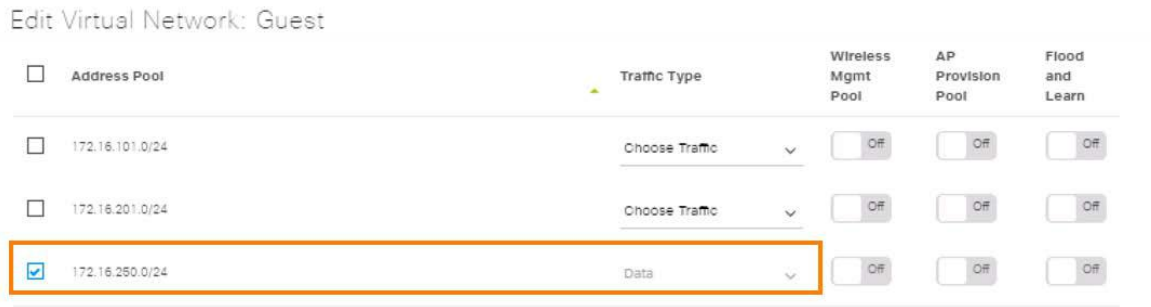
NOTE: 다음 단계로 이동하기 전에 반드시 Save 을 클릭하십시오.

3. **Campus VN** 박스를 클릭하고 2 번째 그림에 나와 있는 내용과 같이 설정합니다. 완료되면 **Update** 를 클릭하십시오.





4. Guest VN 박스를 클릭하고 다음 테이블의 정보에 맞춥니다. Update 를 클릭하십시오.



5. 가상 네트워크에 IP Pool 을 적용한 후, 결과 구성(Configuration)이 패브릭 Edge 노드로 푸시되기 위해 Queue 로 들어갑니다.

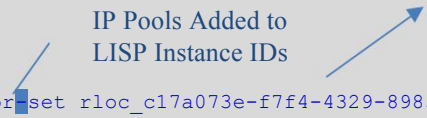
7. 몇 분 후에, 인터페이스의 새로운 running configuration 을 확인합니다. Dot1xClosed 인증 정책이 모든 호스트 인터페이스에 구성되어 있는지 확인 하십시오 .

```
C3850-2#show run | begin 1/0/1
interface GigabitEthernet1/0/1
description Connected to Wired-3 Client
switchport mode access
 switchport voice vlan 4000 device-
 tracking attach-policy IPDT_MAX_10
 authentication control-direction in
 authentication event server dead
action authorize vlan 3999
 authentication event server dead
action authorize voice
 authentication host-mode multi-
 auth authentication order dot1x
 mab authentication priority dot1x
 mab authentication port-control
 auto authentication periodic
 authentication timer reauthenticate server
 authentication timer inactivity server
dynamic
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 description Connected to Guest Client
 switchport mode access
 switchport voice vlan 4000 device-
 tracking attach-policy IPDT_MAX_10
 shutdown
 authentication control-direction in
 authentication event server dead
action authorize vlan 3999
 authentication event server dead
action authorize voice
 authentication host-mode multi-
 auth authentication order dot1x
 mab authentication priority dot1x
 mab authentication port-control
 auto authentication periodic
 authentication timer reauthenticate server
 authentication timer inactivity server
dynamic
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
!
interface GigabitEthernet1/0/3
 switchport mode access
 switchport voice vlan 4000
 device-tracking attach-policy IPDT_MAX_10
 authentication control-direction in
 authentication event server dead
action authorize vlan 3999
 authentication event server dead
action authorize voice
 authentication host-mode multi-
 auth authentication order dot1x
 mab authentication priority dot1x
 mab authentication port-control
 auto authentication periodic
 authentication timer reauthenticate server
 authentication timer inactivity server
dynamic
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
```

이제 IP 어드레스 Pool 이 VN 에 할당되고 장치에 구성되었습니다. 인터페이스는 802.1x Closed 인증 모드로 구성되었습니다. 이제 엔드 포인트를 온보딩시킬 준비가 되었습니다!

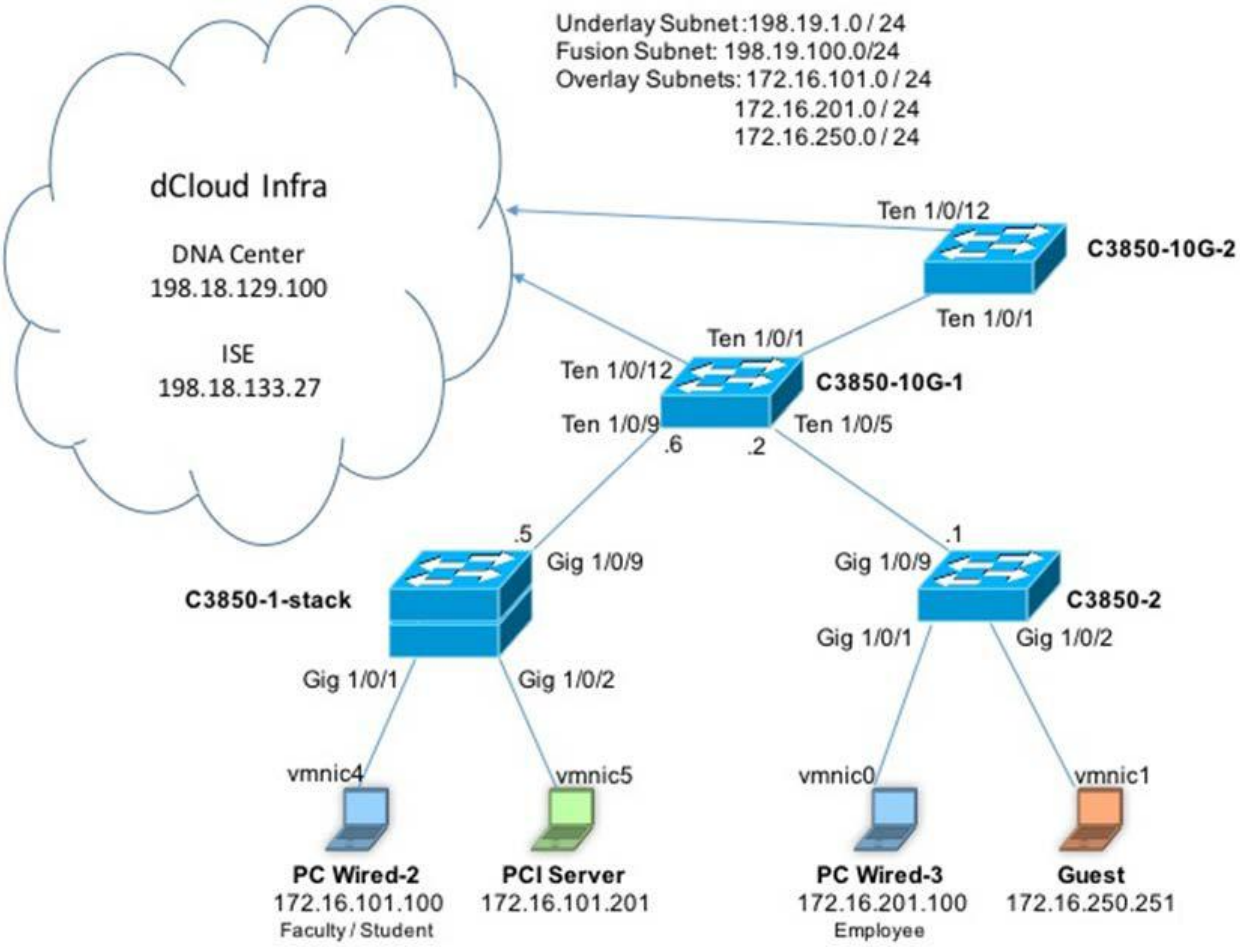
8. C3850-10g-1 및 C3850-2 스위치에서 **show run | sec lisp** 을 실행합니다:

```
Border node (C3850-10g-1):
C3850-10g-1#show run | section
lisp <sniP>
site site_uci
  description map-server configured from apic-em
  authentication-key uci
  eid-record instance-id 4097 0.0.0.0/0 accept-more-specifics
  eid-record instance-id 4098 0.0.0.0/0 accept-more-specifics
  eid-record instance-id 4098 172.16.101.0/24 accept-more-specifics
  eid-record instance-id 4098 172.16.201.0/24 accept-more-specifics
  eid-record instance-id 4099 0.0.0.0/0 accept-more-specifics
  eid-record instance-id 4099 172.16.250.0/24 accept-more-specifics
  exit-site
<snip>

Edge node1 (C3850-2):

C3850-2#show run | section lisp
<snip>
instance-id 4098
  remote-rloc-probe on-route-change
  dynamic-eid 172_16_101_0-Campus
   database-mapping 172.16.101.0/24 locator-set rloc_c17a073e-f7f4-4329-8985-ee73e03e4997
   exit-dynamic-eid
  !
  dynamic-eid 172_16_201_0-Campus
   database-mapping 172.16.201.0/24 locator-set rloc_c17a073e-f7f4-4329-8985-ee73e03e4997
   exit-dynamic-eid
<snip>
```



시나리오 8. SD-Access Inter-Virtual Network 라우팅

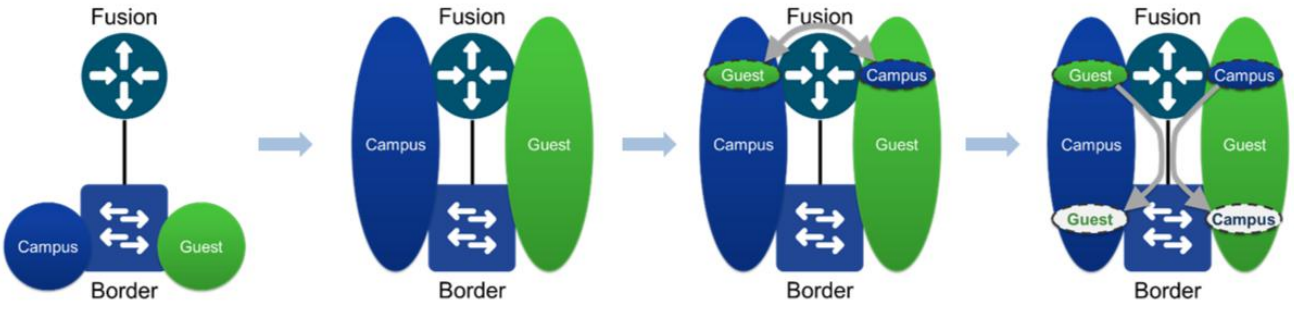
이제 우리는 시나리오의 마지막 부분인 Inter-VN(Inter-Virtual Network) 경로 leaking 작업으로 이동합니다.
이 기능은 퓨전(Fusion) 라우터를 통해 이루어집니다. Lab 구성도 그리고 Campus 및 Guest Virtual 네트워크를 위해 만든 가상 네트워크 및 IP Pool 구성/IP Pool 할당 등을 확인합니다.



각기 다른 Virtual Network 에 속해있는 호스트들이 서로 통신할 수 있도록 다음을 수행합니다:

- 먼저 Border 와 Fusion 라우터 사이에 L3 연결을 생성합니다.
- BGP 를 사용하여 Border 에서 Fusion 라우터 (C3850-1)로 VRF 를 확장합니다.
- 그런 다음 VRF Leaking 을 사용해 퓨전 라우터에 있는 VRF 들간의 경로를 공유합니다
- 마지막으로 VRF 들이 Border 로 향할 수 있도록 경로를 배포 합니다.

완료되면, Fusion 라우터는 다른 VRF 로 트래픽을 Leaking 한 다음, 패브릭 Border 로 보냅니다.
아래 과정을 참조하십시오.

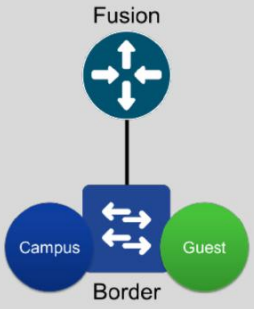


Border 과 Fusion 라우터 사이에 L3 연결 생성

시작하려면 Fabric Border 와 Fusion 라우터 사이의 L3 연결을 생성해야 합니다. 일반적으로 L3 Sub-Interface 링크를 이용합니다. Catalyst 3850 은 Routed Sub-Interface 를 지원하지 않기 때문에 우리는 Fabric Border 와 Fusion 라우터 사이에 SVI 및 L2 trunk 를 사용합니다

1. Catalyst 3850-10g-1 Border 에서 두 개의 VLAN 을 구성하고 C3850-1 Fusion 라우터에 (Ten1/0/1) 연결되는 링크가 새로운 VLAN 을 허용할 수 있도록 Trunk 로 만들면 VN 이 Fusion 라우터로 전송됩니다.

```
C3850-10g-1:


conf t

vlan 901 name
  campus
vlan 902
  name guest

interface TenGigabitEthernet1/0/1
 description 3850-10g-2 1/0/1 Fusion Router
 switchport
 switchport mode trunk
 switchport trunk allowed vlan 901,902
 logging event link-status
 no shut
```



2. 이제 **L3 연결을 위한 SVI 를 만듭니다**.

```
interface vlan 901
  desc Campus to Fusion Router
  vrf forwarding Campus
  ip address 198.19.100.1
  255.255.255.252 no shut

interface vlan 902
  desc Guest to Fusion router
  vrf forwarding Guest
  ip address 198.19.100.5
  255.255.255.252 no shut
```

3. **Border 에서 Fusion 라우터로 VRF 를 Copy 하십시오**. 왜냐하면 RD 와 RT 는 DNA Center 가 자동으로 생성한 숫자이므로 Copy 해서 작업하는걸 권장합니다.

```
COPY YOUR BORDER Campus and Guest VRF CONFIGS TO THE FUSION ROUTER (C3850-10G-
2) (EXAMPLE ONLY…although it is likely yours will match)
vrf definition
 Campus rd 1:4098
 !
 address-family ipv4 route-
 target export 1:4098 route-
 target import 1:4098 exit-
 address-family
!
vrf definition
 Guest rd 1:4099
 !
 address-family ipv4 route-
 target export 1:4099 route-
 target import 1:4099 exit-
 address-family
!
```

4. Fusion 라우터에서 **2 개의 VLAN 을 구성하고** Border 라우터(t1/0/1)에 연결되는 링크를 새로운 VLAN 을 허용하는 Trunk 로 변환하여 Virtual Network 를 Fusion 라우터로 전송할 수 있게 하십시오.

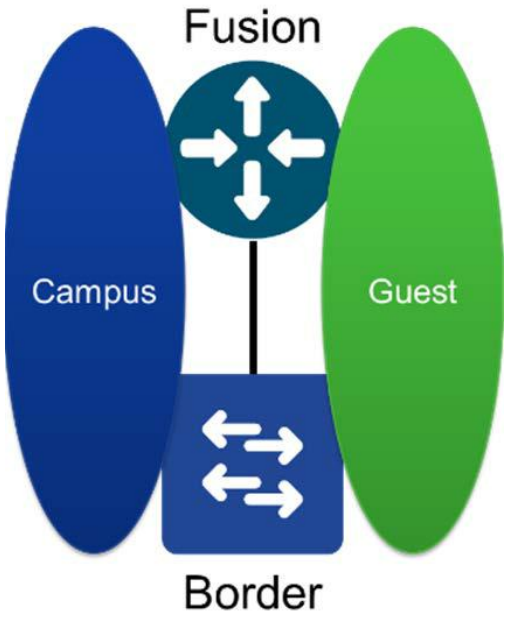
```
C3850-10g-2:


vlan 901 name
  campus
vlan 902
  name guest

interface TenGigabitEthernet1/0/1
 description 3850-10g-1 Ten1/0/1 Border
 switchport trunk allowed vlan 901,902
 switchport mode trunk
 no shut
```

5. 이제는 **L3** 연결을 위해 **SVI** 를 만듭니다

```
interface vlan 901 desc
  fusion to Campus vrf
  forwarding Campus
  ip address 198.19.100.2
  255.255.255.252 no shut

interface vlan 902 desc
  fusion to Guest vrf
  forwarding Guest
  ip address 198.19.100.6
  255.255.255.252 no shut
```

BGP 를 사용하여 Border 에서 Fusion 라우터로 VRF 를 확장.

FCS 에서는 SD-Access 환경을 외부 네트워크와 연결하기 위한 라우팅 프로토콜로 BGP 만 지원합니다. 따라서 다른 프로토콜들이 지원될 때까지 우선 BGP 를 사용해 Production 환경에서 어떻게 동작할지에 대해 개념을 검증합니다.



1. Border 에서 **BGP** 를 구성하고 각 Virtual Network 에 대한 VRF 를 정의합니다.

노트: 서브넷 마스크는 172.16.0.0/16 네트워크를 사용하기 때문에 BGP 가 일반적으로 광고하는 / 16 대신 / 24 를 광고하도록 합니다

```
C3850-10g-1:


router bgp 65004
  address-family ipv4 vrf Campus
    network 172.16.101.0 mask 255.255.255.0
    network 172.16.201.0 mask 255.255.255.0
    neighbor 198.19.100.2 remote-as 65003
    neighbor 198.19.100.2 update-source Vlan901
```

```
    neighbor 198.19.100.2 activate
    exit

  address-family ipv4 vrf Guest
    network 172.16.250.0 mask 255.255.255.0
    neighbor 198.19.100.6 remote-as 65003
    neighbor 198.19.100.6 update-source Vlan902
    neighbor 198.19.100.6 activate
    exit
```

2. 그리고 Null0 인터페이스를 사용하여 강제로 라우팅 테이블에 올라갈 수 있도록 경로를 정적으로 정의해야 합니다.

```
C3850-10g-1:


ip route vrf Campus 172.16.101.0 255.255.255.0 Null0
ip route vrf Campus 172.16.201.0 255.255.255.0 Null0
ip route vrf Guest 172.16.250.0 255.255.255.0 Null0
```

3. 현재 Campus 및 Guest VRF 에 경로가 존재하는지 확인합니다.

```
C3850-10g-1#show ip route vrf Campus

Routing Table: Campus
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su -
       IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter
       area, * - candidate default, U - per-user static route o - ODR, P -
       periodic downloaded static route, H - NHRP, l - LISP a - application
       route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 2 subnets
S        172.16.101.0 is directly connected, Null0
S172.16.201.0 is directly connected, Null0 198.19.100.0/24 is
      variably subnetted, 2 subnets, 2 masks
C198.19.100.0/30 is directly connected, Vlan901
L198.19.100.1/32 is directly connected, Vlan901


C3850-10g-1#show ip route vrf Guest

Routing Table: Guest
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su -
       IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter
       area, * - candidate default, U - per-user static route o - ODR, P -
       periodic downloaded static route, H - NHRP, l - LISP
```

```
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 1 subnets
S        172.16.250.0 is directly connected, Null0
      198.19.100.9/24 is variably subnetted, 2 subnets, 2 masks
C198.19.100.4/30 is directly connected, Vlan902
L198.19.100.5/32 is directly connected, Vlan902
```

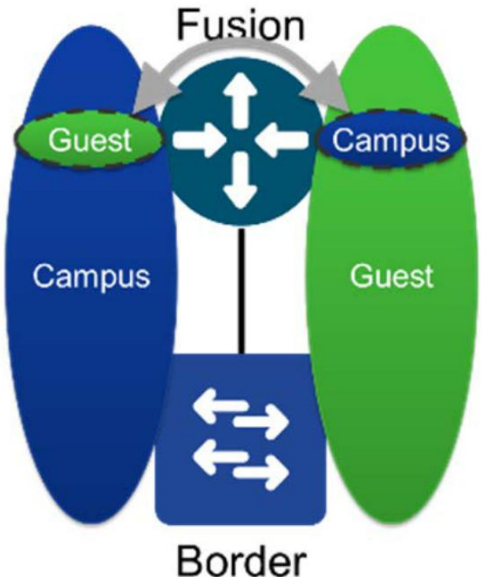
4. 앞서 Border 에서 구성한 것처럼, Fusion 라우터에서 BGP 를 구성하고 각 Virtual Network 에 대한 VRF 를 정의합니다

```
C3850-10g-2:



router bgp 65003 address-family
  ipv4 vrf Campus
    neighbor 198.19.100.1 remote-as 65004
    neighbor 198.19.100.1 update-source
    Vlan901 neighbor 198.19.100.1 activate
  exit

  address-family ipv4 vrf Guest
    neighbor 198.19.100.5 remote-as 65004
    neighbor 198.19.100.5 update-source Vlan902
    neighbor 198.19.100.5 activate
  exit
```

NOTE: 퓨전 라우터에는 정적 경로는 필요하지 않습니다.

VRF leaking 을 사용하여 Fusion 라우터에서 경로 공유

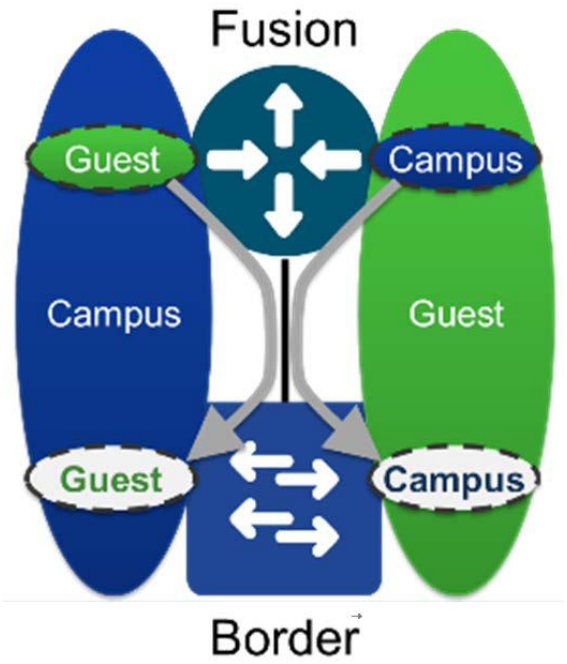
1. Border 구성에서 Route-target 을 Copy 하기 위해 Fusion 라우터에서 VRF Route leaking 을 사용합니다.



```
EXAMPLE ONLY
C3850-10-2(config-router)#vrf definition Campus
C3850-10-2(config-vrf)# address-family ipv4
C3850-10-2(config-vrf-af)# route-target import 1:4099
C3850-10-2(config-vrf)#vrf definition Guest
C3850-10-2(config-vrf-af)# address-family ipv4
C3850-10-2(config-vrf)# route-target import 1:4098


C3850-10-2 (config-vrf-af)#do sho ip route vrf Campus

Routing Table: Campus
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su -
       IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter
       area, * - candidate default, U - per-user static route o - ODR, P -
       periodic downloaded static route, H - NHRP, l - LISP a - application
       route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 3 subnets
B        172.16.101.0 [20/0] via 198.19.100.1, 00:03:53
B        172.16.201.0 [20/0] via 198.19.100.1, 00:03:49
B        172.16.250.0 [20/0] via 198.19.100.5 (Guest), 00:00:10
      198.19.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.19.100.0/30 is directly connected, Vlan901
L        198.19.100.2/32 is directly connected, Vlan901

C3850-1(config-vrf)#do sho ip route vrf Guest

Routing Table: Guest
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su -
       IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter
       area, * - candidate default, U - per-user static route o - ODR, P -
       periodic downloaded static route, H - NHRP, l - LISP a - application
       route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 3 subnets
B        172.16.101.0 [20/0] via 198.19.100.1 (Campus), 00:00:23
B        172.16.201.0 [20/0] via 198.19.100.1 (Campus), 00:00:23
B        172.16.250.0 [20/0] via 198.19.100.6, 00:01:28
      198.19.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.19.100.4/30 is directly connected, Vlan902
L        198.19.100.6/32 is directly connected, Vlan902
```

Fusion 라우터에서 Border 로 경로 배포

일반적으로 경로는 라우터간에 자동으로 분배됩니다. 하지만 이 구성에서는 Border 의 BGP 가 Leaking 된 경로를 학습하지 않습니다. 왜냐하면 Leaking 된 VRF 로 향하는 AS 경로가 Border 를 다시 가리키기 때문입니다. 이 문제를 해결하기 위해 allow as-in 명령어를 사용하여 BGP 가 경로 학습을 차단하지 못하게 합니다.



1. Border 의 BGP 가 경로를 허용하도록 합니다.

```
C3850-10g-1# show run | sec bgp
router bgp 65004
 bgp log-neighbor-changes
 !
 address-family ipv4 vrf Campus
  network 172.16.101.0 mask 255.255.255.0
 network 172.16.201.0 mask 255.255.255.0
 neighbor 198.19.100.2 remote-as 65003
 neighbor 198.19.100.2 update-source Vlan901
 neighbor 198.19.100.2 activate exit-
 address-family
 !
 address-family ipv4 vrf Guest
  network 172.16.250.0 mask 255.255.255.0
 neighbor 198.19.100.6 remote-as 65003
 neighbor 198.19.100.6 update-source Vlan902
 neighbor 198.19.100.6 activate exit-
 address-family


C3850-10g-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router bgp 65004
   address-family ipv4 vrf Campus
   neighbor 198.19.100.2 allowas-in
```

```
    neighbor 198.19.100.6 allowas-in
    end

C3850-10g-1#show bgp all
For address family: IPv4 Unicast

For address family: VPNv4 Unicast

BGP table version is 7, local router ID is 192.168.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 Route Distinguisher: 1:16123729 (default for vrf Guest)
  *>  172.16.101.0/24  198.19.100.6                           0 65003 65004 i
  *>  172.16.201.0/24  198.19.100.6                           0 65003 65004 i
  *>  172.16.250.0/24  0.0.0.0                  0         32768 i
 Route Distinguisher: 1:1467079553 (default for vrf Campus)
  *>  172.16.101.0/24  0.0.0.0                  0         32768 i
  *>  172.16.201.0/24  0.0.0.0                  0         32768 i
  *>  172.16.250.0/24  198.19.100.2                          0 65003 65004 i


C3850-10g-1#show ip route vrf Campus

Routing Table: Campus
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su -
       IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter
       area, * - candidate default, U - per-user static route o - ODR, P -
       periodic downloaded static route, H - NHRP, l - LISP a - application
       route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 3 subnets
S        172.16.101.0 is directly connected, Null0
S172.16.201.0 is directly connected, Null0
B172.16.250.0 [20/0] via 198.19.100.2, 00:20:53 198.19.100.0/24
      is variably subnetted, 2 subnets, 2 masks
C198.19.100.0/30 is directly connected, Vlan901
L198.19.100.1/32 is directly connected, Vlan901


C3850-10g-1#sho ip route vrf Guest

Routing Table: Guest
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP a -
       application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 3 subnets
B        172.16.101.0 [20/0] via 192.168.254.5, 02:09:25
B        172.16.201.0 [20/0] via 192.168.254.5, 02:09:25
S        172.16.250.0 is directly connected, Null0
      198.19.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.19.100.4/30 is directly connected, Vlan902
L        198.19.100.5/32 is directly connected, Vlan902
```