온보드 NFVIS WAN 에지 디바이스

목차

소개

이 문서에서는 관리 및 운영을 위해 NFVIS 지원 시스템을 Catalyst™ SD-WAN 환경에 온보딩하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco SDWAN
- 엔에프비스
- 플러그 앤 플레이(PNP)

다음과 같이 가정합니다.

- SD-WAN 컨트롤러(vManage, vBond, vSmart)가 유효한 인증서로 이미 구축되어 있습니다.
- Cisco WAN Edge(이 경우 NFVIS)는 WAN 전송 전반의 공용 IP 주소를 통해 연결할 수 있는 vBond 오케스트레이터 및 기타 SD-WAN 컨트롤러에 연결할 수 있습니다
- NFVIS 버전은 Control Components Compatibility Guide를 준수해야 합니다.

사용되는 구성 요소

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.

하드웨어

- C8300-UCPE-1N20(그러나 모든 NFVIS 지원 플랫폼에 적용 가능)

소프트웨어

- vManage 20.14.1
- vSmart & vBond 20.14.1
- NFVIS 4.14.1

PnP 워크플로

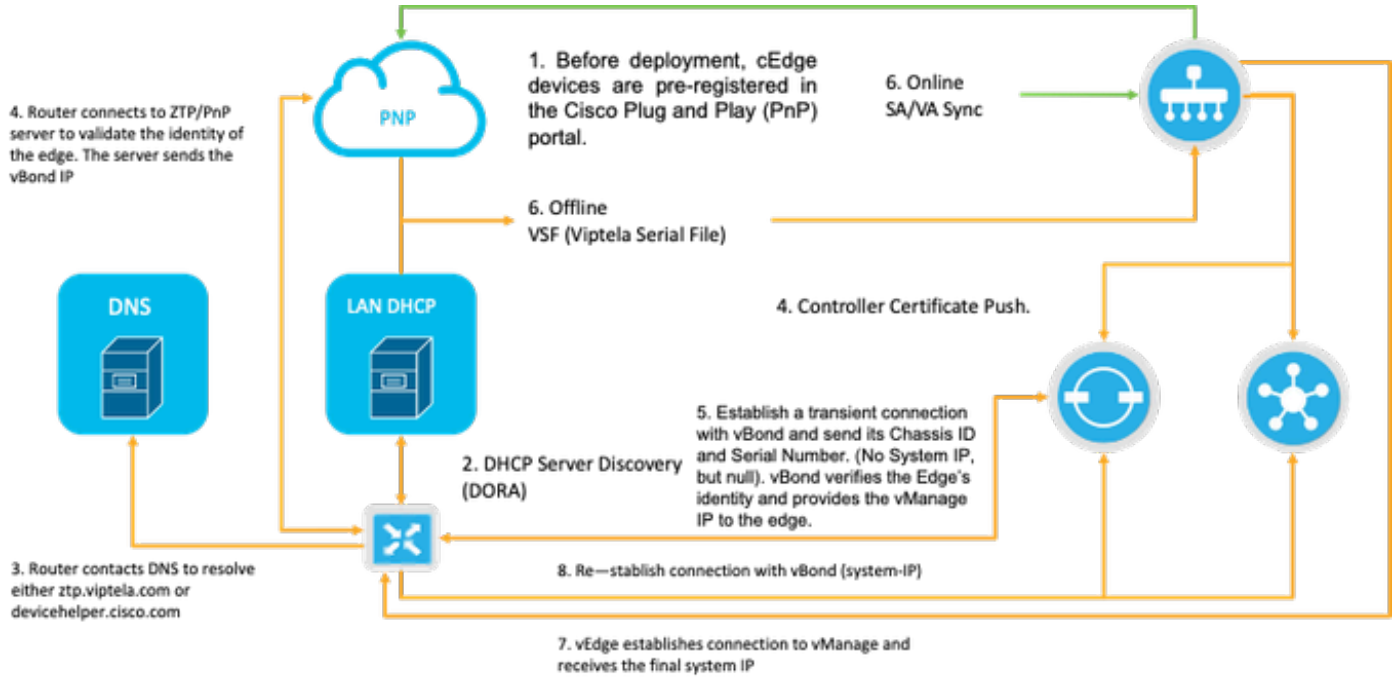
WAN 에지 디바이스의 신뢰는 제조에 사전 로드되거나, 수동으로 로드되거나, vManage에 의해 자동으로 배포되거나, PnP 또는 ZTP 자동 배포 프로비저닝 프로세스 중에 설치되는 루트 체인 인증서를 사용하여 수행됩니다.

SD-WAN 솔루션은 허용 목록 모델을 사용합니다. 즉, SDWAN 오버레이 네트워크에 가입할 수 있는 WAN 에지 디바이스를 모든 SD-WAN 컨트롤러에서 미리 알아야 합니다. 이 작업은 PnP(Plug-and-Play Connect Portal)(https://software.cisco.com/software/pnp/devices)에서 WAN Edge 디바이스를 추가하여 수행됩니다

이 절차에서는 항상 디바이스를 식별하고 신뢰할 수 있으며 동일한 오버레이 네트워크에 허용 목록에 나열해야 합니다. 동일한 오버레이 네트워크에서 SD-WAN 구성 요소 간에 보안 제어 연결을 설정하기 전에 모든 SD-WAN 구성 요소 간에 상호 인증이 수행되어야 합니다. WAN 에지 디바이스의 ID는 섀시 ID 및 인증서 일련 번호로 고유하게 식별됩니다. WAN 에지 라우터에 따라 인증서는 여러 가지 방법으로 제공됩니다.

- 하드웨어 기반 vEdge: 인증서는 제조 중에 설치된 온보드 TPM(Tamper Proof Module) 칩에 저장됩니다.
- 하드웨어 기반 Cisco IOS®-XE SD-WAN: 인증서는 제조 중에 설치된 온보드 SUDI 칩에 저장된다.
- 가상 플랫폼 또는 Cisco IOS-XE SD-WAN 장치: 디바이스에 루트 인증서(예: ASR1002-X 플랫폼)가 미리 설치되어 있지 않습니다. 이러한 디바이스의 경우 SD-WAN 컨트롤러로 디바이스를 인증하기 위해 vManage에서 OTP(One-Time Password)를 제공합니다.

ZTP(Zero Touch Provisioning)를 수행하려면 DHCP 서버를 사용할 수 있어야 합니다. 그렇지 않은 경우 PnP(Plug and Play) 프로세스의 나머지 단계를 진행하기 위해 IP 주소를 수동으로 할당할 수 있습니다.



도 1. PnP 및 WAN 에지 디바이스 트러스트 워크플로 다이어그램

NFVIS 지원 디바이스의 보안 온보딩

SN 및 인증서 일련 번호 검색

NFVIS 지원 하드웨어의 하드웨어 기반 SUDI(Secure Unique Device Identifier) 칩은 인증된 디바이스만 SD-WAN Manager 오케스트레이터에 안전한 TLS 또는 DTLS 제어(평면 터널)를 설정할 수 있도록 하는 데 사용됩니다. support show chassis executive level 명령을 사용하여 해당 일련 번호를 수집합니다.

```
C8300-UCPE-NFVIS# support show chassis
Product Name              : C8300-UCPE-1N20
Chassis Serial Num        : XXXXXXXXX
Certificate Serial Num    : XXXXXXXXXXXXXXXXX
```

PnP 포털에 디바이스 추가

https://software.cisco.com/software/pnp/devices으로 이동하여 사용자 또는 랩 환경에 맞는 올바른 Smart Account 및 Virtual Account를 선택합니다. (이름이 여러 Smart Account인 경우 도메인 식별자로 구분할 수 있습니다.)

사용자 또는 사용자가 어떤 SA(Smart Account)/VA(Virtual Account)를 사용해야 할지 모를 경우, "Device Search" 텍스트 링크에서 항상 기존/온보딩된 일련 번호를 검색하여 해당 SA/VA가 속한 SA/VA를 확인할 수 있습니다.

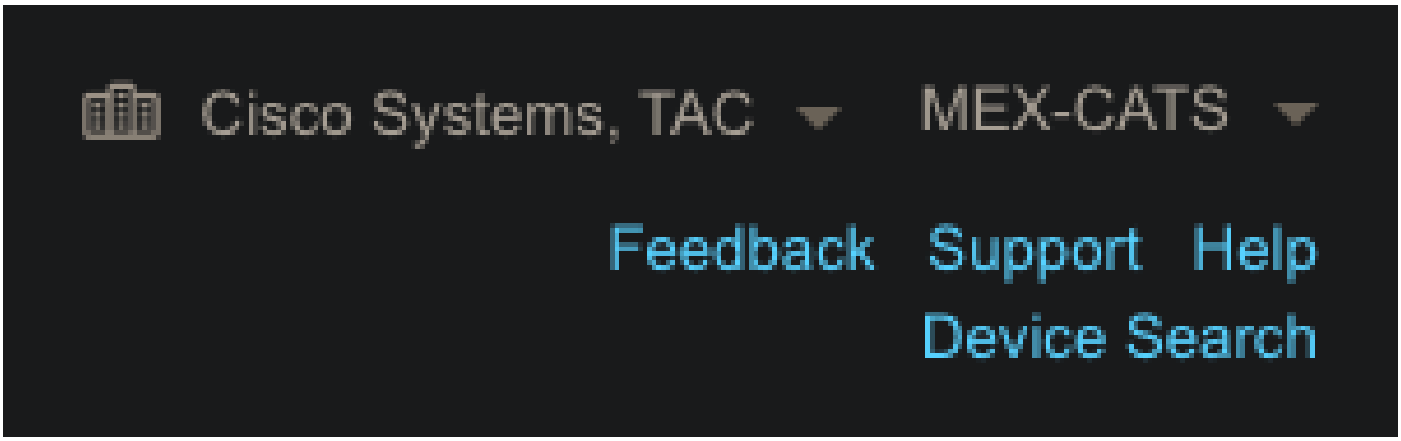


그림 2. SA/VA 선택 및 디바이스 검색 버튼.

올바른 SA/VA를 선택했으면 "Add Devices...(디바이스 추가...)"를 클릭합니다.

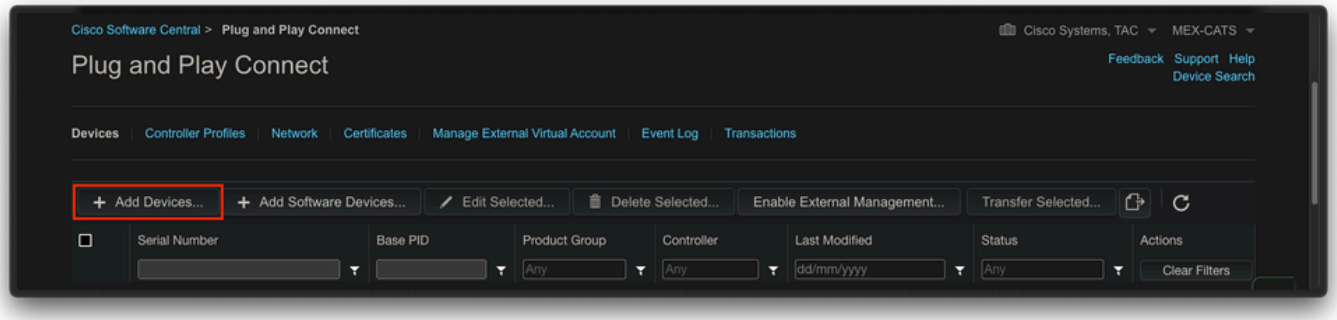


그림 3. "디바이스 추가..." 버튼을 클릭하여 물리적 디바이스 등록을 확인합니다.

이 경우에는 하나의 장치만 온보딩하므로 수동 입력만으로도 충분합니다.

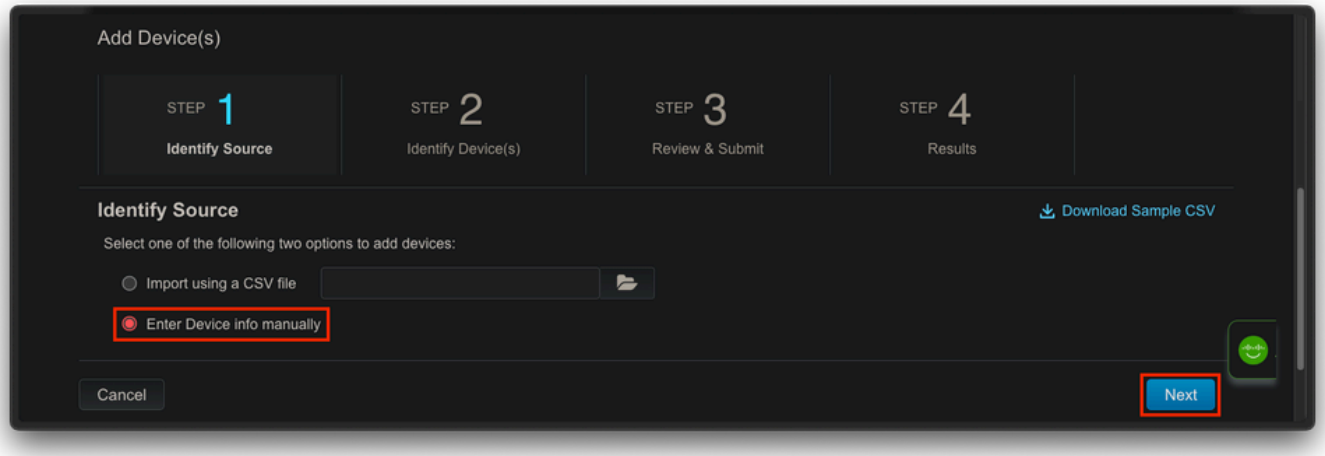


그림 4. 장치 정보 입력, 수동(개별) 또는 CSV(다중)에 대한 "장치 추가..." 대안.

2단계에서 "+ Identify Device...(디바이스 식별...)" 버튼을 클릭합니다. 양식 모달이 나타납니다. NFVIS의 support show chassis 출력 정보에 표시된 정보를 자세히 입력하고 해당 vBond 컨트롤러 프로필을 선택합니다.

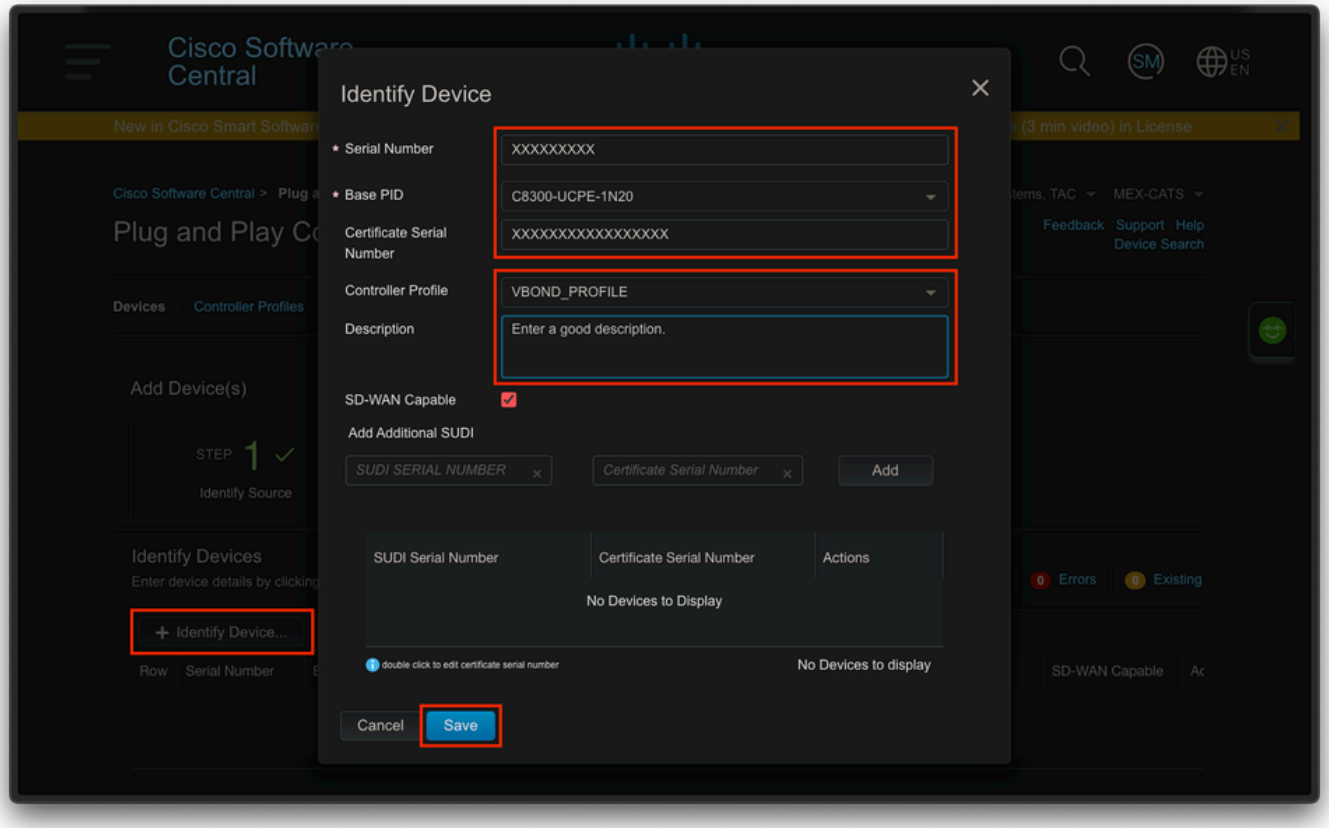


그림 5. 장치 식별 양식.

저장했으면 3단계의 Next(다음)를 클릭하고 4단계의 Submit(제출)을 클릭합니다.

Nfvis의 PnP

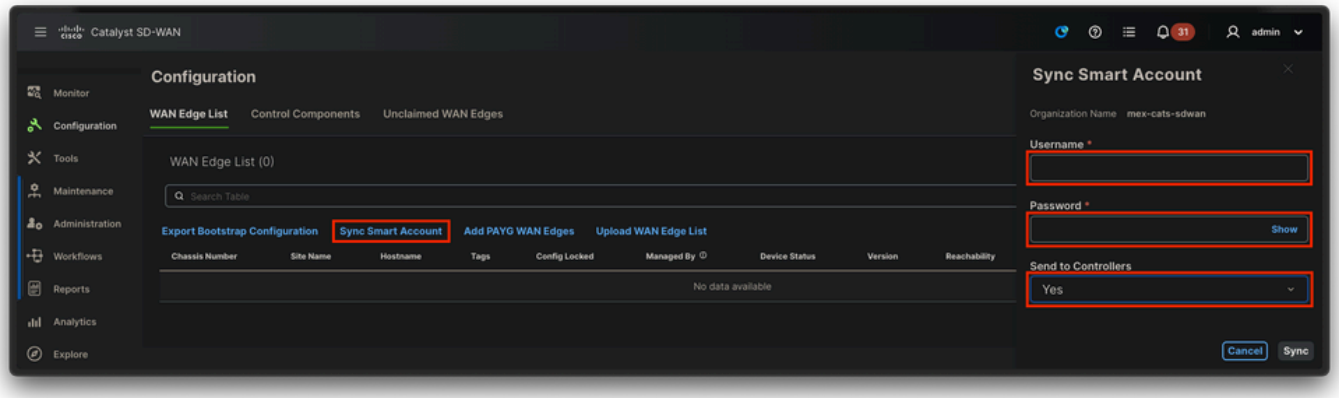
자동 모드와 정적 모드를 모두 포함하는 NFVIS 내의 PnP에 대한 다양한 컨피그레이션 설정에 대한 자세한 내용은 NFVIS PnP 명령 리소스를 참조하십시오.

PnP는 모든 NFVIS 버전에서 기본적으로 활성화되어 있습니다.

PnP를 사용한 vManage 동기화

온라인 모드

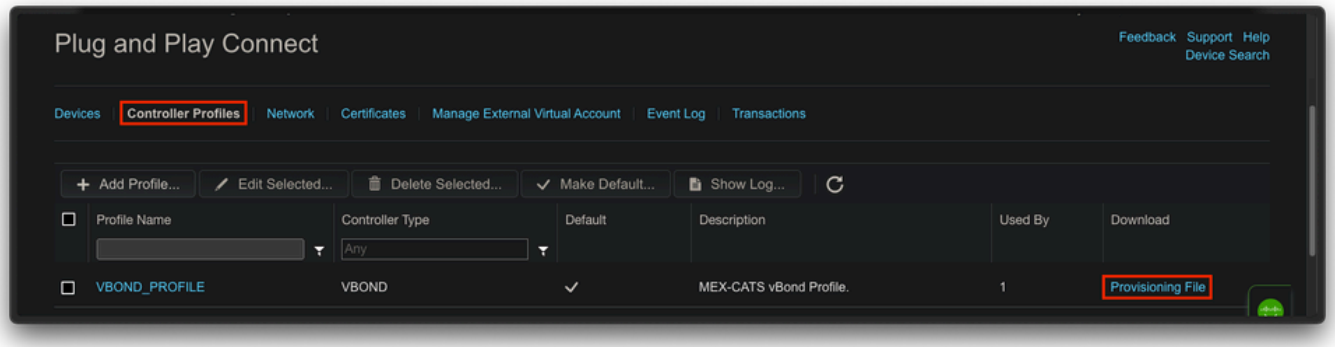
vManage에서 인터넷 및 PnP 포털에 연결할 수 있는 경우 SA/VA 동기화만 수행할 수 있어야 합니다. 이를 위해 Configuration(컨피그레이션) > Devices(디바이스)로 이동하고 Sync Smart Account(Smart Account 동기화)를 나타내는 텍스트 버튼을 클릭합니다. Cisco Software Central 로그인에 사용되는 자격 증명이 필요합니다. 모든 컨트롤러에 인증서 푸시를 전송해야 합니다.



도 6. SA/VA 동기화를 통한 WAN 에지 라우터 업데이트.

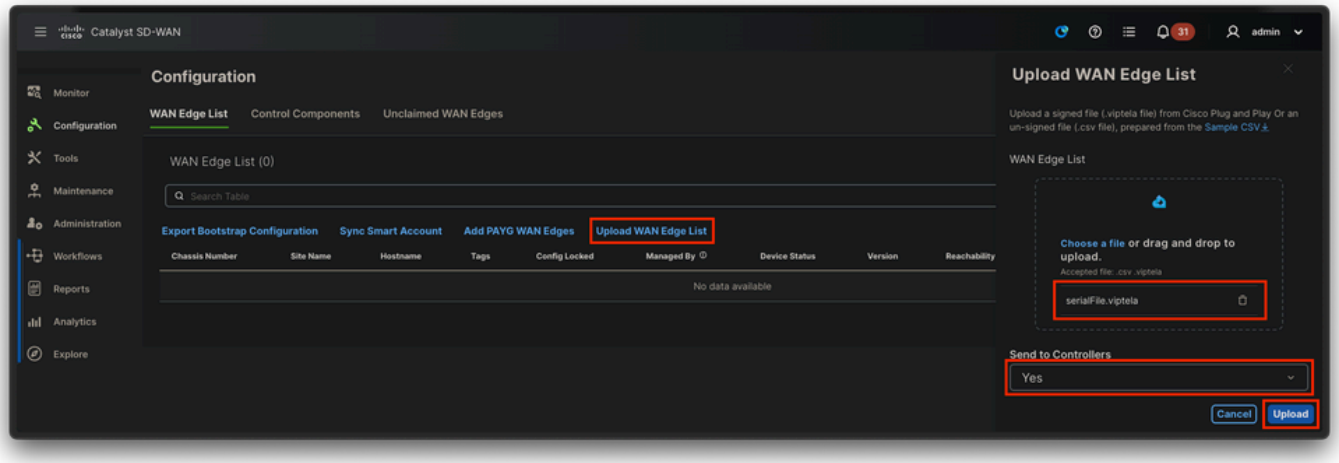
오프라인 모드

vManage가 랩 환경에 있거나 인터넷 액세스 권한이 없는 경우, 디바이스 목록에 추가된 SN을 포함해야 하는 프로비저닝 파일을 PnP에서 수동으로 업로드할 수 있습니다. 이 파일은 .viptela(Viptela Serial File) 유형이며 "Controller Profiles" 탭에서 가져올 수 있습니다.



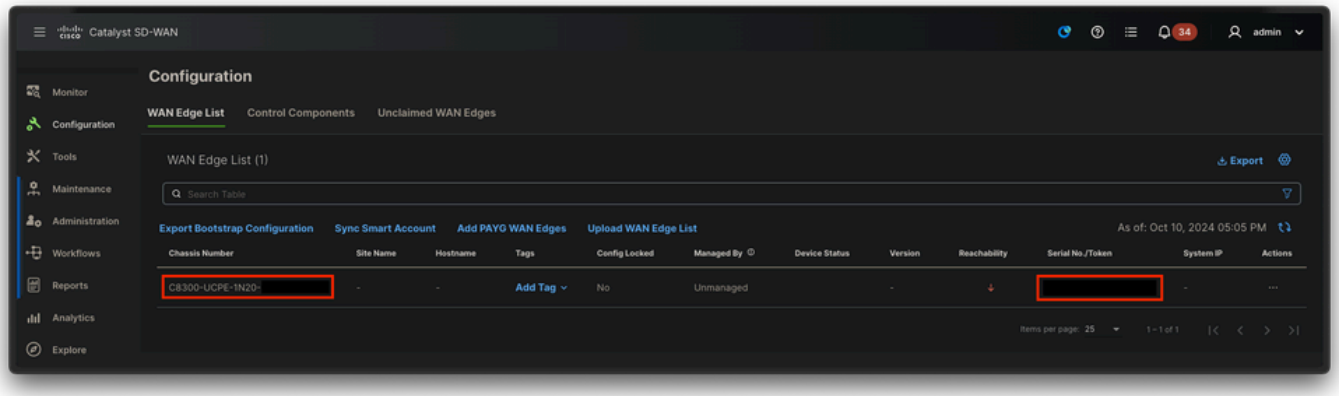
도 7은 CEdge WAN 리스트 업데이트를 위한 파일 다운로드를 프로비저닝하는 것입니다.

프로비저닝 파일의 수동 업로드를 위해 Configuration(컨피그레이션) > Devices(디바이스)로 이동하고 Upload WAN Edge List(WAN 에지 목록 업로드)를 나타내는 텍스트 버튼을 클릭합니다. 해당 파일을 끌어서 놓을 수 있는 사이드바가 나타납니다. 이러한 작업이 수행된 후 업로드 버튼이 강조 표시되지 않으면 파일 선택을 클릭하고 팝업 파일 탐색기 창에서 파일을 수동으로 검색합니다. 모든 컨트롤러에 인증서 푸시를 전송해야 합니다.



도 8. PnP 포털에서 다운로드한 프로비저닝 파일(VSF, Viptela Serial File)을 이용한 WAN 리스트 업데이트.

Online(온라인) 또는 Offline(오프라인) 방법을 완료한 후 WAN Edge List(WAN 에지 목록) 테이블에서 PnP에 등록된 디바이스의 SN에 해당하는 디바이스 항목을 볼 수 있어야 합니다.

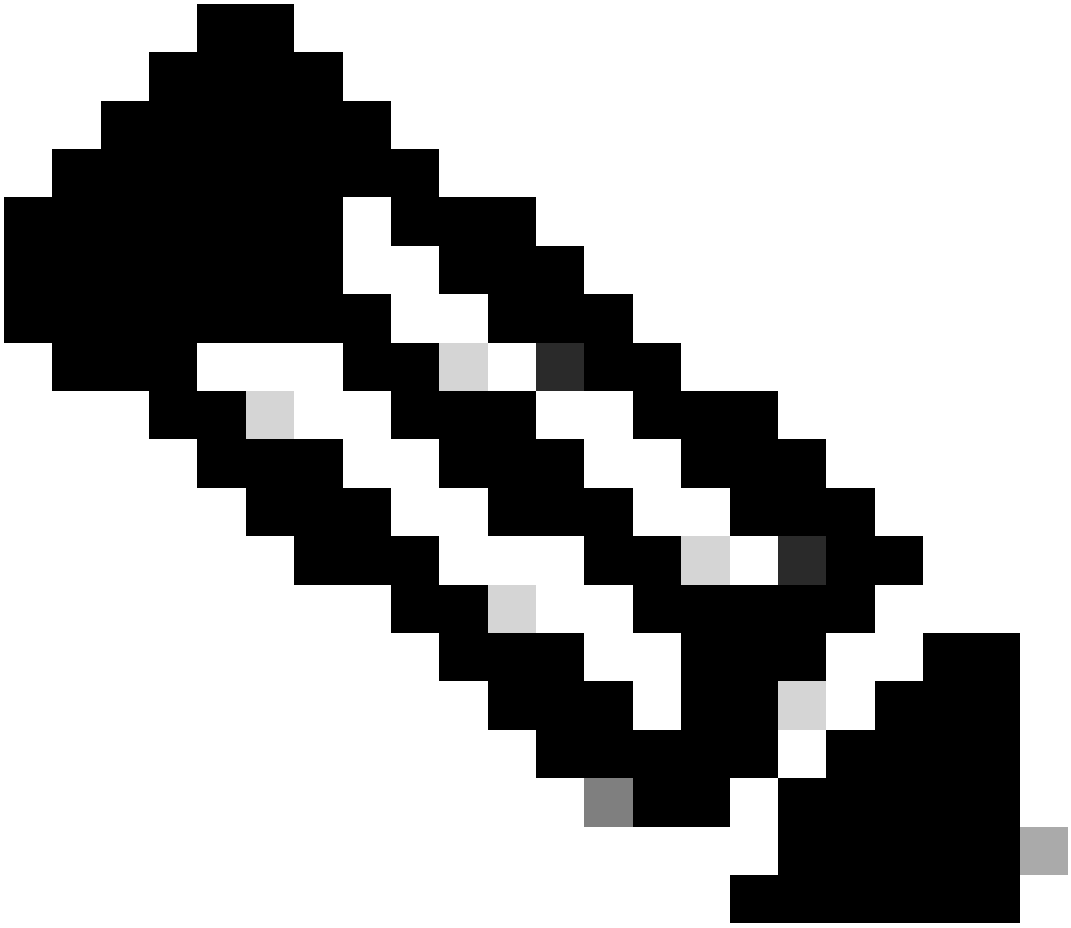


도 9의 8300 디바이스는 에지 리스트 내에 있다.

NFVIS 자동 온보딩 및 제어 연결

NFVIS에서 devicehelper.cisco.com을 확인할 수 있는 경우(인터넷을 통해 PnP에 연결) 온보딩이 자동으로 수행됩니다. 온보딩된 NFVIS 시스템은 기본 컨트롤러 정보가 포함된 viptela-system:system 및 vpn 0 컨피그레이션을 자동으로 표시합니다.

Cisco NFVIS Release 4.9.1부터는 관리 포트를 통해 관리 플레인에 대한 제어 연결을 설정하는 것이 지원됩니다. 컨트롤 플레인에 정상적으로 연결하려면 SD-WAN Manager를 사용하여 관리 포트에 연결할 수 있어야 합니다.



참고: "system" 키워드가 포함된 모든 명령은 system:system으로 작성해야 합니다. 완료에 탭 키를 사용하면 이 새 표준에 자동으로 적용됩니다.

```
C8300-UCPE-NFVIS# show running-config viptela-system:system
viptela-system:system
 admin-tech-on-failure
 no vrrp-advt-with-phymac
 sp-organization-name "Cisco Systems"
 organization-name "Cisco Systems"
 vbond
```

```
port 12346 logging disk enable ! ! ntp parent no enable stratum 5 exit ! !
```

VPN 0은 SD-WAN 솔루션의 사전 정의된 전송 VPN입니다. 삭제하거나 수정할 수 없습니다. 이 VPN의 목적은 WAN 전송 네트워크(언더레이)와 네트워크 서비스(오버레이) 간의 분리를 적용하는 것입니다.

```
C8300-UCPE-NFVIS# show running-config vpn 0
vpn 0
 interface wan-br
  no shutdown
  tunnel-interface
   color gold
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   encapsulation ipsec
  !
 !
!
```

제어 연결은 SD-WAN 패브릭의 서로 다른 노드(컨트롤러 및 에지 라우터) 간에 설정된 DTLS 세션입니다. NFVIS는 라우팅 결정을 담당하는 라우팅 플랫폼이 아니므로 vSmarts와의 제어 연결을 구성하지 않습니다. 기본적으로 vManage에 대해 "과제" 상태를 관찰할 수 있습니다.

```
C8300-UCPE-NFVIS# show control connection
                                                                                    PEER
PEER    PEER PEER            SITE       DOMAIN PEER                                 PRIV  PEER
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                           PORT  PUBLIC IP
-------------------------------------------------------------------------------------------------
vbond   dtls 0.0.0.0         0          0      10.88.247.79                         12346 10.88.247.
vmanage dtls 10.10.10.10     100        0      10.88.247.71                         12946 10.88.247.
```

이는 일반적으로 system-ip가 없고, organization-name이 잘못되었거나 전혀 구성되지 않았음을 나타냅니다. PnP 포털 및 vBond에서 조직 이름을 설정하고 vManage와의 제어 연결이 설정되면 합니다. 그렇지 않은 경우 템플릿에 해당 system-ip 및 site-id를 사용하여 NFV Config-Group(20.14.1부터 지원됨) 내에서 이 정보를 푸시하거나, viptela-system:system 하위 컨피그레이션 내에서 정적으로 구성합니다.

```
C8300-UCPE-NFVIS#(config)# viptela-system:system
C8300-UCPE-NFVIS#(config-viptela-system:system)# system-ip
```

```
C8300-UCPE-NFVIS#(config-viptela-system:system)# site-id

C8300-UCPE-NFVIS#(config-viptela-system:system)# organization-name

C8300-UCPE-NFVIS#(config-viptela-system:system)# commit Commit complete.
```

이러한 항목은 vManage에서 찾을 수 있습니다.

- 조직 이름: 관리 > 설정 > 시스템 > 조직 이름
- 검사기 IP 및 포트: 관리 > 설정 > 시스템 > 검사기

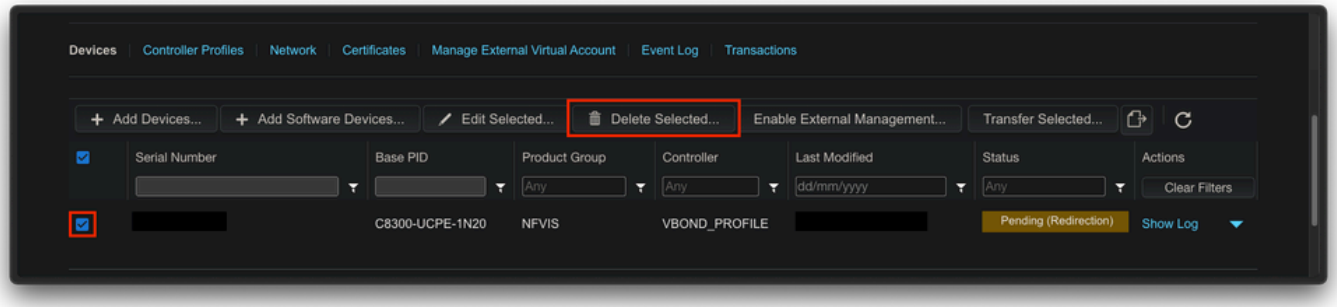
나머지 컨피그레이션을 viptela-system:system 하위 컨피그레이션에 입력한 후 활성/설정된 제어 연결이 필요합니다.

```
C8300-UCPE-NFVIS# show control connections
                                                                                    PEER
PEER    PEER PEER            SITE       DOMAIN PEER                                PRIV  PEER
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                          PORT  PUBLIC IP
-------------------------------------------------------------------------------------------------
vbond   dtls 0.0.0.0         0          0      10.88.247.79                        12346 10.88.247.
vmanage dtls 10.10.10.10     100        0      10.88.247.71                        12946 10.88.247.
```

NFVIS 관리 해제

NFVIS를 "관리되지 않음" 상태로 되돌리려면 다음 작업을 수행해야 합니다.

1. PnP 포털에서 디바이스 항목을 제거합니다.



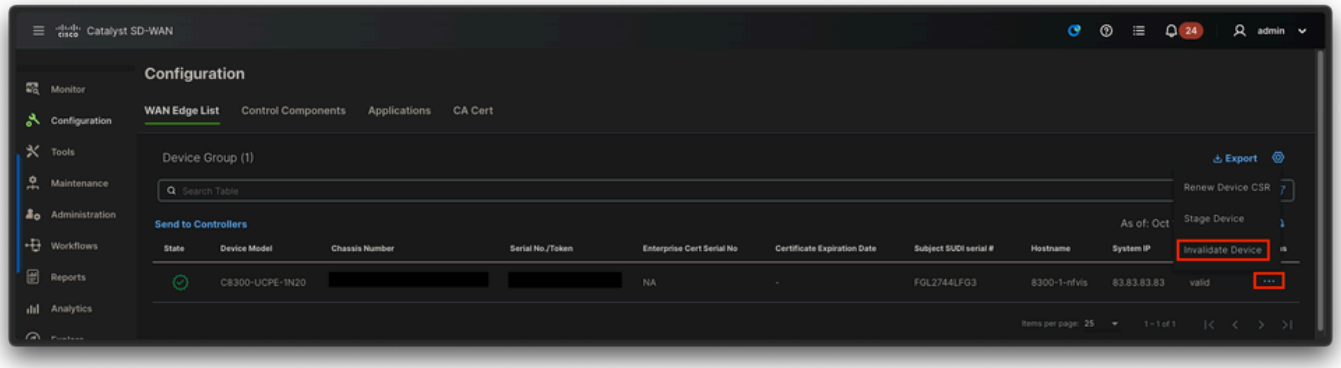
도 10. 8300 PnP 포털에서 디바이스 제거

2. 공장 초기화 NFVIS.

```
C8300-UCPE-NFVIS# factory-default-reset all
```

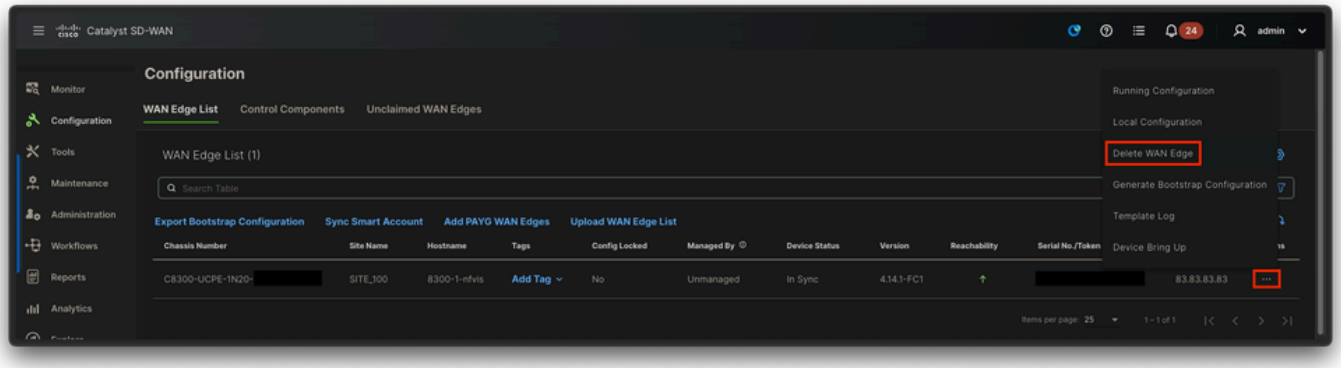
3. 선택적 단계: vManage Edge 목록에서 디바이스를 제거합니다.

3.1 디바이스 인증서를 무효화합니다.



도 11. 8300 인증서 무효화

3.2 WAN 에지 목록에서 디바이스를 삭제합니다.



도 12. 8300 WAN 에지 목록에서 제거.

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.