

cEdge 라우터에 UTD 보안 가상 이미지 설치

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[Cisco IOS XE SDWAN 소프트웨어를 실행하는 라우터\(16.x\)](#)

[Cisco IOS XE Software를 실행하는 라우터\(17.x\)](#)

[구성](#)

[1단계. 가상 이미지 업로드](#)

[2단계. 디바이스 템플릿에 보안 정책 및 컨테이너 프로파일 하위 템플릿 추가](#)

[3단계. 보안 정책 및 컨테이너 프로파일로 디바이스 템플릿 업데이트 또는 첨부 다음을 확인합니다.](#)

[일반적인 문제](#)

[문제 1. 오류: 다음 장치에 컨테이너 소프트웨어 서비스가 없습니다.](#)

[문제점 2. 사용 가능한 메모리가 부족합니다.](#)

[문제 3. 잘못된 참조](#)

[문제 4. UTD가 설치되어 있고 활성화되어 있지만 활성화되지 않았습니다.](#)

[관련 정보](#)

소개

이 문서에서는 Cisco IOS XE SD-WAN 디바이스에서 보안 기능을 활성화하기 위해 UTD(Unified Threat Defense) 보안 가상 이미지를 설치하는 방법에 대해 설명합니다.

사전 요구 사항

- 이러한 기능을 사용하기 전에 관련 보안 가상 이미지를 vManage 리포지토리에 업로드하십시오.
- cEdge 라우터는 템플릿이 미리 연결된 vmanage 모드여야 합니다.
- IPS(Intrusion Prevention System), IDS(Intrusion Detection System), URL 필터링(URL-F) 또는 AMP(Advanced Malware Protection) 필터링을 위한 보안 정책 템플릿을 생성합니다.

요구 사항

- 4000 Integrated Services Router Cisco IOS XE SD-WAN(ISR4k)
- 1000 Integrated Services Router Cisco IOS XE SD-WAN(ISR1k)
- 1000v 클라우드 서비스 라우터(CSR1kv),
- 1000v ISRv(Integrated Services Router)
- 8GB DRAM을 지원하는 cEdge 플랫폼입니다.

사용되는 구성 요소

- Cisco UTD 가상 이미지
- vManage 컨트롤러
- 컨트롤러와 제어 연결이 있는 cEdge 라우터

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.

배경 정보

Cisco UTD 이미지는 디바이스 템플릿에 보안 정책을 설치해야 하며, cEdge 라우터의 IPS(Intrusion Prevention System), IDS(Intrusion Detection System), URL 필터링(URL-F), AMP(Advanced Malware Protection) 등의 보안 기능이 활성화되어 있어야 합니다.

소프트웨어 Cisco에서 Cisco UTD Snort IP Engine [소프트웨어 다운로드](#)

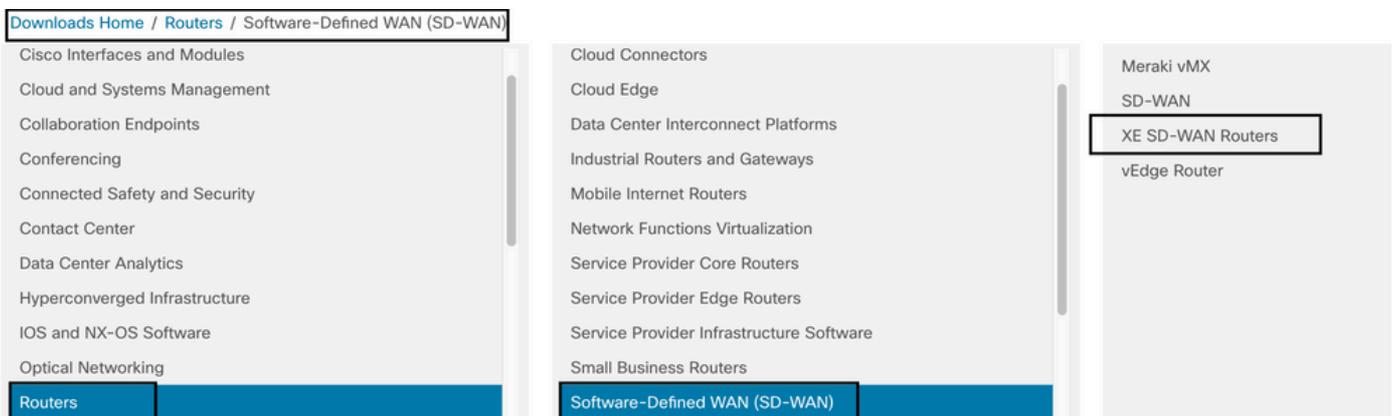
현재 Cisco IOS XE 버전에서는 Cisco UTD 가상 이미지 지원 regex를 사용합니다. 권장 및 지원되는 **UTD 이미지**를 검증하려면 show utd engine standard version 명령을 사용합니다.

```
Router01# show utd engine standard version
IOS-XE Recommended UTD Version: 1.0.13_SV2.9.16.1_XE17.3
IOS-XE Supported UTD Regex: ^1\.0\.[([0-9]+)_SV(.*)_XE17.3$
```

참고 이미지를 다운로드할 경로는 라우터가 Cisco IOS XE SDWAN 소프트웨어(16.x) 또는 범용 Cisco IOS XE 소프트웨어(17.x)를 실행하는지에 따라 다릅니다.

Cisco IOS XE SDWAN 소프트웨어를 실행하는 라우터(16.x)

Cisco UTD Snort IPS Engine 소프트웨어를 다운로드할 수 있는 경로는 라우터/SD-WAN(Software-Defined WAN)/XE SD-WAN 라우터 및 Series Integrated Router입니다.



cEdge 라우터의 모델 유형을 선택합니다.

참고 UTD 기능에는 ASR(Series Aggregation Services Router)을 사용할 수 없습니다.

The screenshot shows a navigation menu on the left with 'Routers' selected. The main content area is divided into three columns: 'Meraki vMX', 'SD-WAN', and 'vEdge Router'. The 'XE SD-WAN Routers' link is highlighted. To the right, a list of router series is shown, including 'ASR 1000 Series IOS XE SD-WAN', 'CSR 1000V Series IOS XE SD-WAN', 'ISR 1000 Series IOS XE SD-WAN', and 'ISR 4000 Series IOS XE SD-WAN'.

유형 라우터 모델을 선택한 후 **Cisco IOS XE SD-WAN 소프트웨어 옵션**을 선택하여 16.x 버전의 cEdge용 UTD 패키지를 가져옵니다.

Select a Software Type

[IOS XE In-Service Software Upgrade \(ISSU\) Matrix](#)

[IOS XE SD-WAN Software](#)

[IOS XE Software](#)

참고 cEdges 라우터용 16.x 코드의 Cisco UTD 가상 이미지를 선택하는 다운로드 경로에는 **Cisco IOS XE 소프트웨어 옵션**도 표시됩니다. 이는 17.x에 대해서만 cEdge의 업그레이드 코드를 선택하는 경로이지만, 버전 17.x에 대한 UTD 가상 이미지는 없습니다. Cisco Unified Regular Cisco IOS XE 및 Cisco IOS XE SDWAN 코드는 17.x 및 최신 버전이므로 17.x용 Cisco UTD 가상 이미지를 가져오는 경로는 일반 Cisco IOS XE 코드와 동일합니다.

cEdge의 현재 버전을 선택하고 해당 버전의 UTD 패키지를 다운로드합니다.

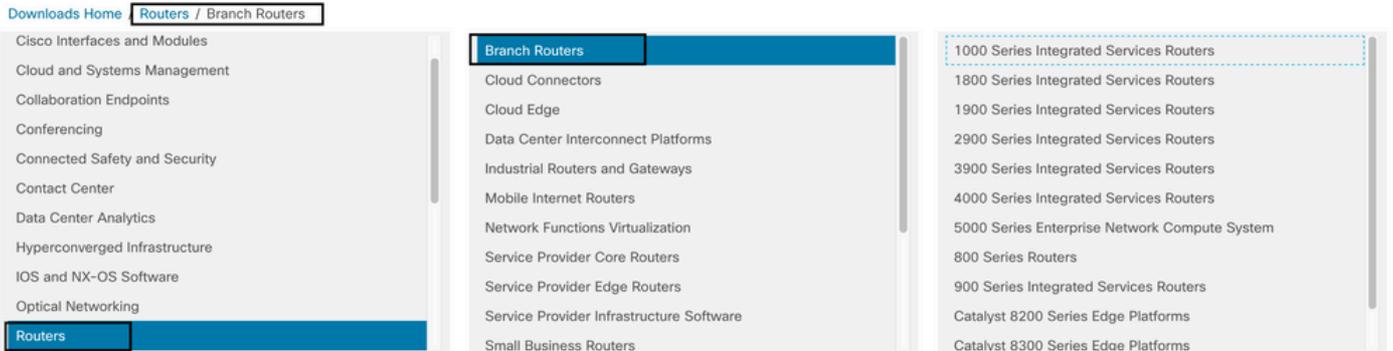
The screenshot shows the 'ISR 4000 Series IOS XE SD-WAN' page for release 16.12.5 MD. On the left, a search bar and a list of release options are visible, with '16.12.5(MD)' selected. The main content area displays a table of software packages with columns for 'File Information', 'Release Date', and 'Size'. The 'UTD Engine for IOS XE SD-WAN' package is highlighted.

File Information	Release Date	Size
Cisco ISR 4200 Series IOS XE SD-WAN Software isr4200-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	482.84 MB
Cisco ISR 4300 Series IOS XE SD-WAN Software isr4300-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	557.83 MB
Cisco ISR 4400 Series IOS XE SD-WAN Software isr4400-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	621.88 MB
Cisco ISR 4400v2 Series IOS XE SD-WAN Software isr4400v2-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	623.49 MB
UTD Engine for IOS XE SD-WAN secapp-ucmk9.16.12.05.1.0.18_SV2.9.16.1_XE16.12.x86_64.tar Advisories	29-Jan-2021	52.01 MB

Cisco IOS XE Software를 실행하는 라우터(17.x)

Cisco IOS XE 릴리스 17.2.1r 및 최신 버전에서는 universalk9 이미지를 사용하여 Cisco IOS XE SD-WAN 및 Cisco IOS XE를 Cisco IOS XE 디바이스에 모두 구축합니다.

UTD Snort IPS Engine 소프트웨어는 **Routers > Branch Routers > Series Integrated Router**에 있습니다.



라우터의 모델 유형을 선택한 후 UTD Snort IPS Engine Software를 선택합니다.

Software Download

Downloads Home / [Routers](#) / [Branch Routers](#) / [4000 Series Integrated Services Routers](#) / [4221 Integrated Services Router](#)



라우터의 현재 버전을 선택하고 선택한 버전에 대한 UTD 패키지를 다운로드합니다.

Software Download

Downloads Home / Routers / Branch Routers / 4000 Series Integrated Services Routers / 4221 Integrated Services Router / UTD Short IPS Engine Software- 17.7.1a

4221 Integrated Services Router

Release 17.7.1a

Related Links and Documentation
- No related links or documentation -

File Information	Release Date	Size
UTD Engine OVA for 17.7.1 release iosxe-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.ova Advisories	30-Nov-2021	147.72 MB
UTD Engine for IOS XE secapp-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.tar Advisories	30-Nov-2021	52.51 MB

참고: 비디오 코드 대신 Cisco IOS XE Software를 실행하는 Cisco ISR1100X Series 라우터 (Cisco Nutella Routers SR1100X-4G/6G)는 x86_x64를 기반으로 합니다. ISR4K용으로 게시된 Cisco UTD 가상 이미지가 이 라우터에서 작동합니다. 현재 Cisco IOS XE SDWAN 버전에 대해 지원되는 동일한 Cisco UTD 이미지 코드 버전을 Nutella 라우터에 설치할 수 있습니다. 권장 및 지원되는 regex Cisco UTD 이미지를 검증하려면 show utd engine standard version 명령을 사용합니다.

구성

1단계. 가상 이미지 업로드

가상 이미지가 cEdge의 현재 Cisco IOS XE SDWAN 코드와 일치하는지 확인하고 vmanage 리포지토리에 업로드합니다.

Maintenance(유지 관리) > Software Repository(소프트웨어 저장소) > Virtual Image(가상 이미지) > Upload Virtual Image(가상 이미지 업로드) > vManage로 이동합니다.

MAINTENANCE | SOFTWARE REPOSITORY

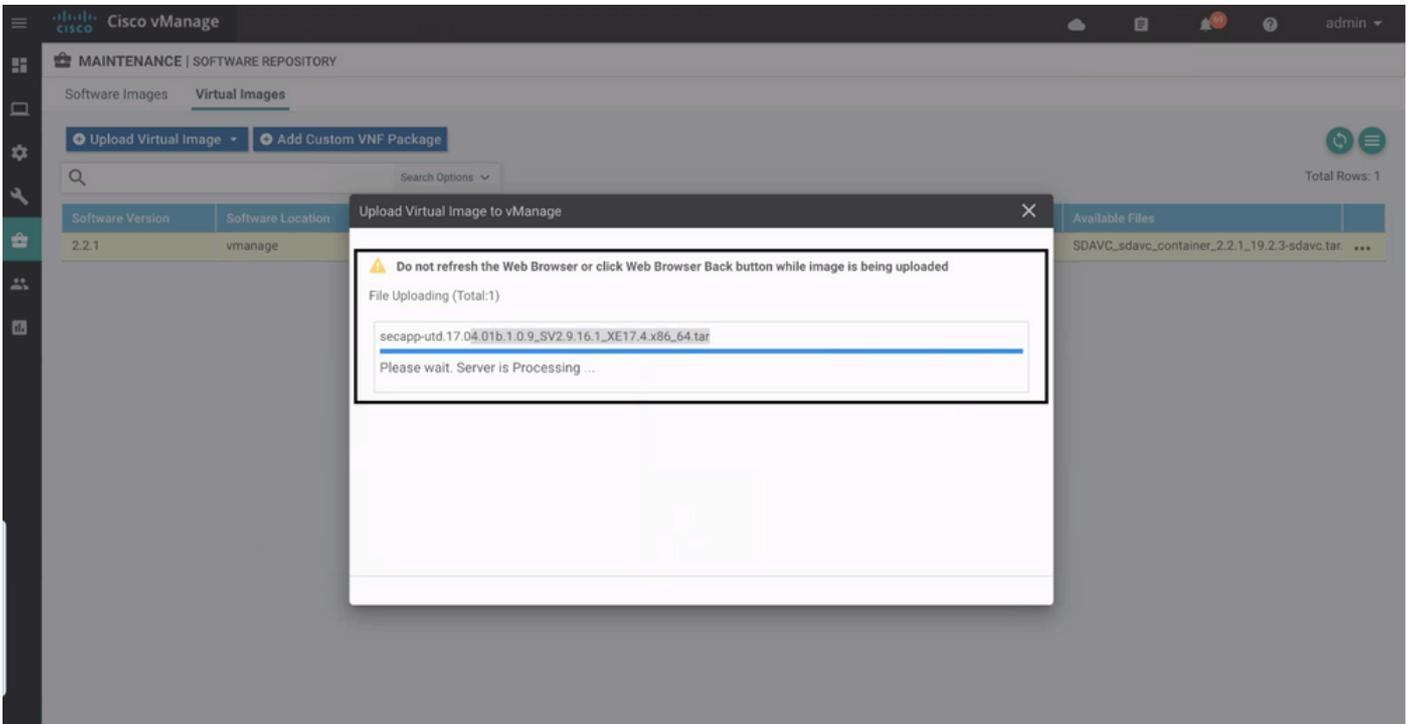
Software Images **Virtual Images**

Upload Virtual Image **Add Custom VNF Package**

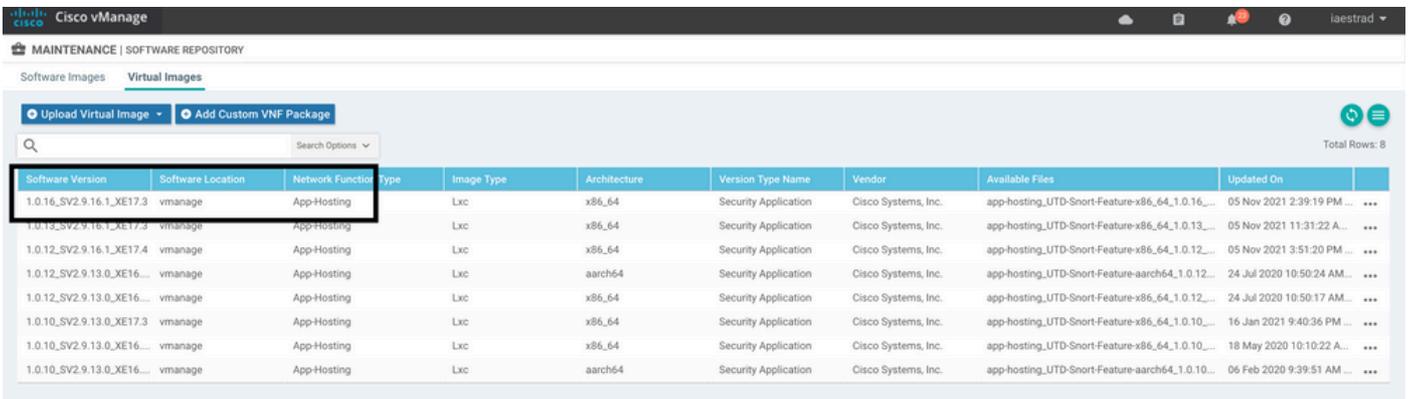
vManage
Remote Server - vManage

Search Options

Software Version Software Location Network Function Type

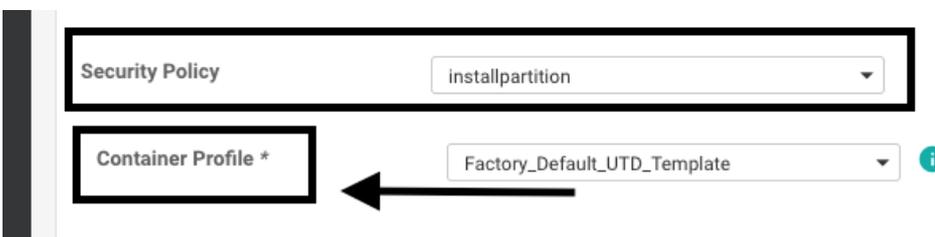


Cisco UTD 가상 이미지가 성공적으로 업로드되면 저장소에 있는지 다시 확인합니다.



2단계. 디바이스 템플릿에 보안 정책 및 컨테이너 프로파일 하위 템플릿 추가

이전에 생성한 보안 정책을 디바이스 템플릿에 추가합니다. 보안 정책에는 디바이스 템플릿에 대한 IPS/IDS, URL-F 또는 AMP 필터링 정책이 있어야 합니다. 컨테이너 프로파일을 자동으로 엽니다. 기본 컨테이너 프로파일을 사용하거나 필요한 경우 수정합니다.



3단계. 보안 정책 및 컨테이너 프로필로 디바이스 템플릿 업데이트 또는 첨부

템플릿을 업데이트하거나 cEdge 라우터에 연결합니다. 컨피그레이션 차이에 IPS/IDS, URL-F 또는 AMP 필터링 기능에 대한 앱 호스팅 컨피그레이션 및 UTD 엔진이 구성되었음을 확인합니다.

```
258 app-hosting appid utd
259 app-resource package-profile cloud-low
260 app-vnic gateway0 virtualportgroup 0 guest-interface 0
261 guest-ipaddress 192.168.1.2 netmask 255.255.255.252
262 !
263 app-vnic gateway1 virtualportgroup 1 guest-interface 1
264 guest-ipaddress 192.0.2.2 netmask 255.255.255.252
265 !
266 start
267 !
258 268 !ldp run
259 269 nat64 translation timeout tcp 60
260 270 nat64 translation timeout udp 1
271 utd multi-tenancy
272 utd engine standard multi-tenancy
273 threat-inspection profile GPC_IPS_v06_copy_copy
274 threat detection
275 policy security
276 logging level warning
277 !
278 utd global
279 !
280 !
281 policy
282 no app-visibility
283 no flow-visibility
284 no implicit-acl-logging
285 log-frequency 1000
286 !
```

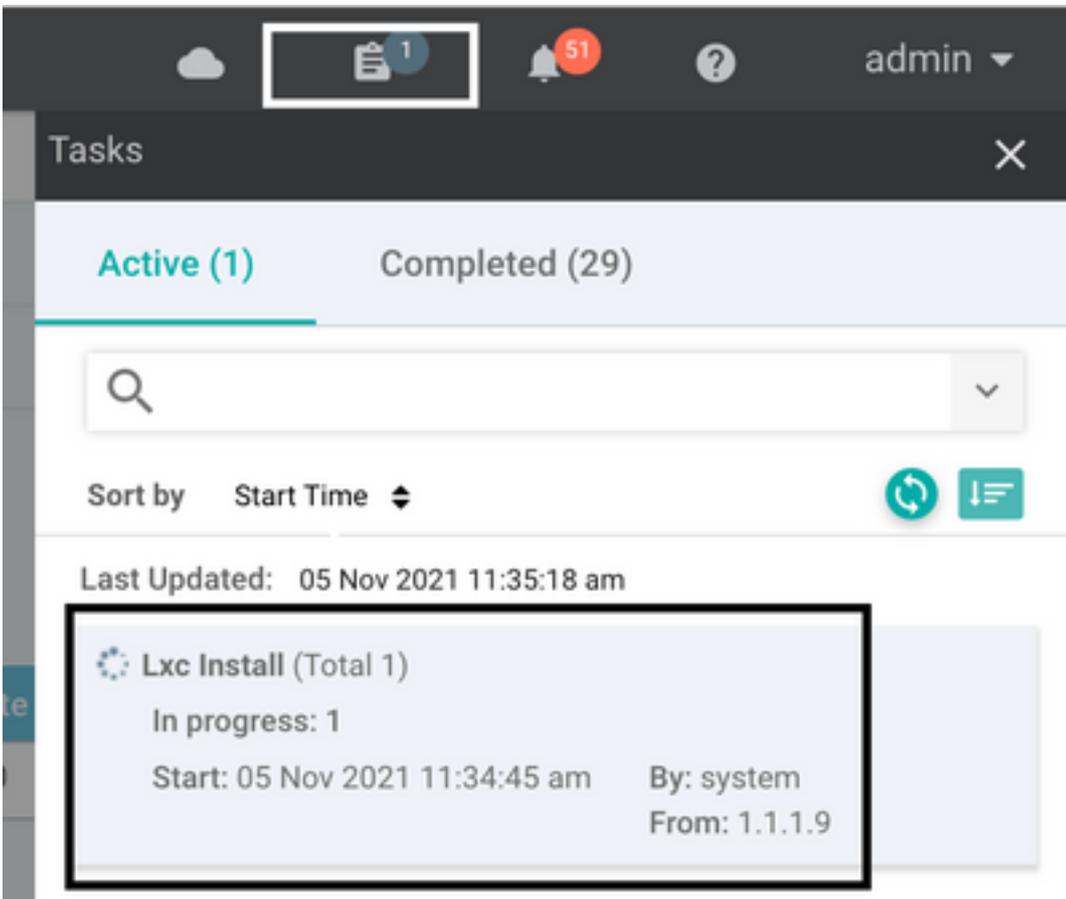
vmanage에서 적용된 컨피그레이션에 UTD 엔진 기능이 있음을 발견하여 템플릿 상태가 Done-scheduled로 변경되었습니다. 따라서 vmanage는 cEdge에서 UTD 보안 기능을 사용하려면 가상 이미지를 설치해야 한다고 판단합니다.

Push Feature Template Configuration | Validation Success

Total Task: 1 | Done - Scheduled : 1

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID
Done - Scheduled	Device needs to install some ap...	CSR-FDCDD4AE-4DB9-B79B-8FF...	CSR1000v	ZBFWTest	70.70.70.1	70

템플릿이 일정 상태로 이동하면 작업 메뉴에 **진행 중인 새 작업**이 나타납니다. 새로운 작업은 Lxc 설치이며, 이는 새 컨피그레이션을 푸시하기 전에 vmanage가 자동으로 cEdge에 가상 이미지 설치를 시작함을 의미합니다.



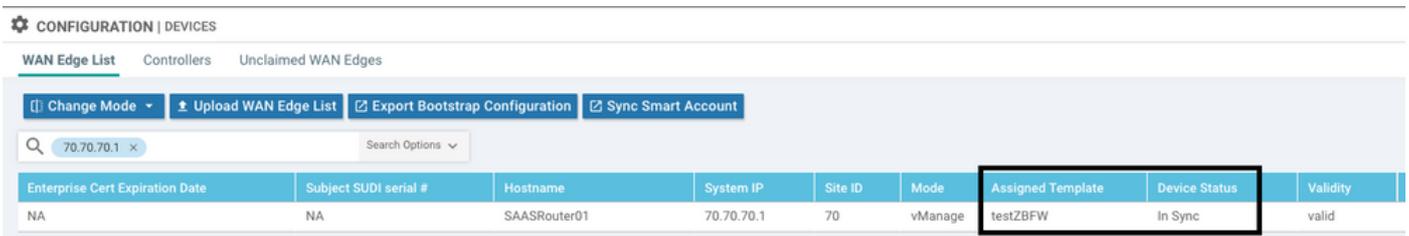
LX 컨테이너가 설치되면 vManage는 UTD 기능을 사용하여 사전 예약 구성을 푸시합니다. 이전에 컨피그레이션이 예약되었기 때문에 이 작업에 대한 새 작업이 없습니다.



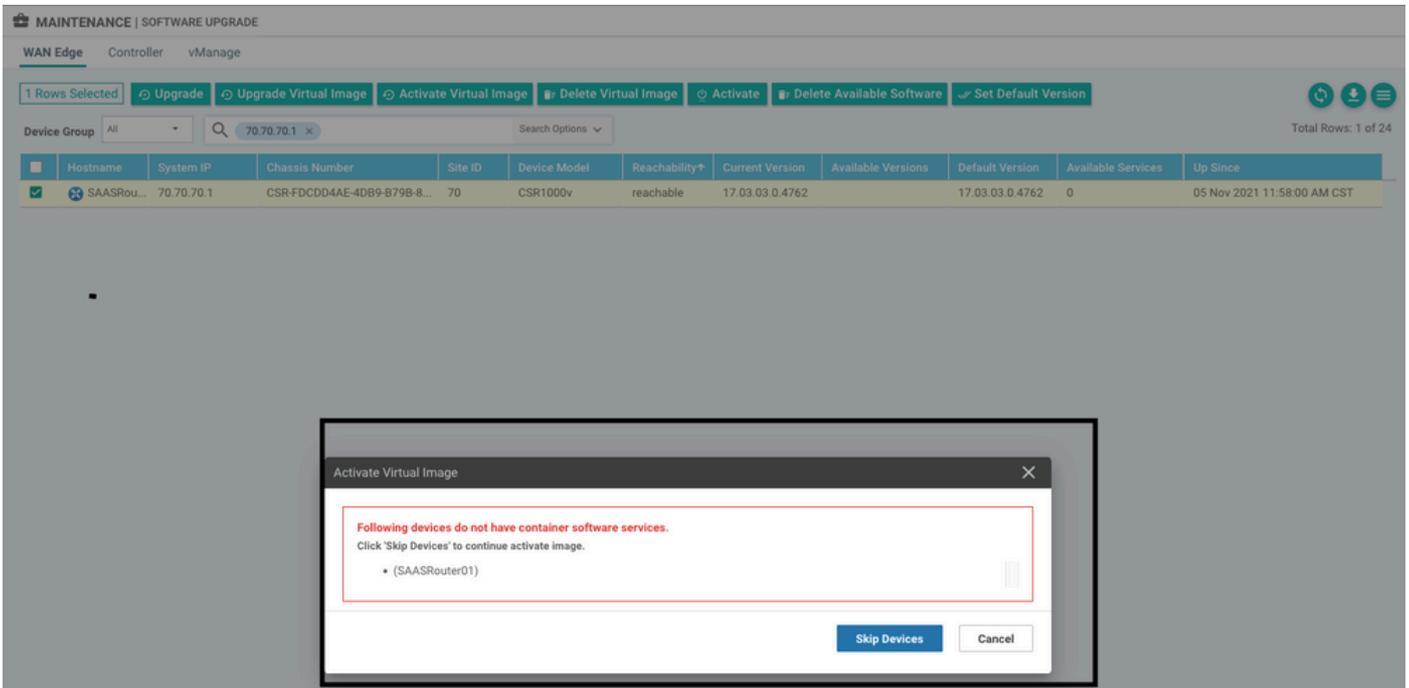
다음을 확인합니다.

cEdge가 vManage 및 연결된 템플릿과 동기화되어 있는지 확인합니다.

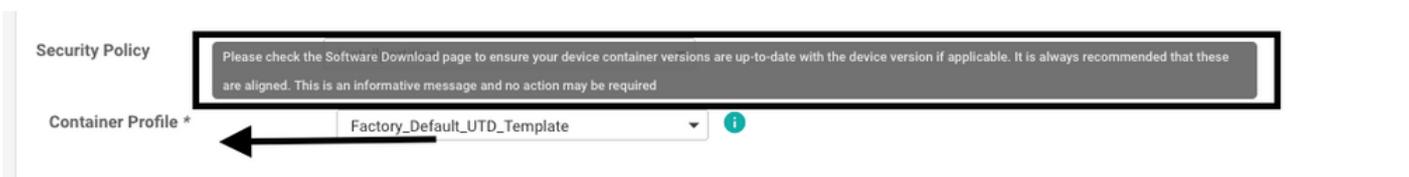
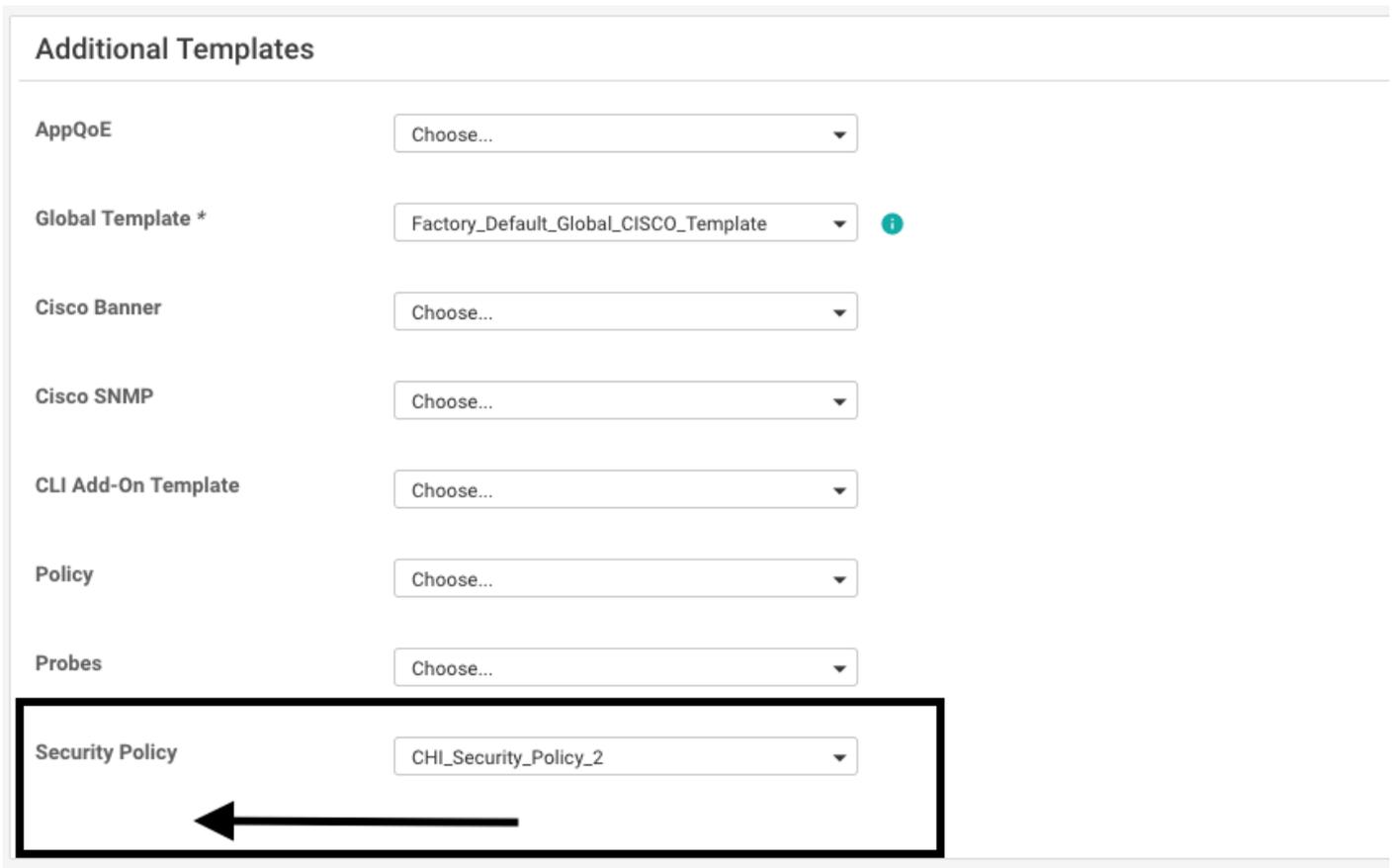
Configuration(컨피그레이션) > Devices(디바이스)로 이동합니다.



Cisco UTD 버전이 설치되어 있는지 확인합니다.



가상 이미지에서 오류를 보냅니다. 선택한 cEdge 라우터에 컨테이너 프로파일 하위 템플릿의 보안 정책이 없는 경우 디바이스에는 컨테이너 소프트웨어 서비스가 없습니다.



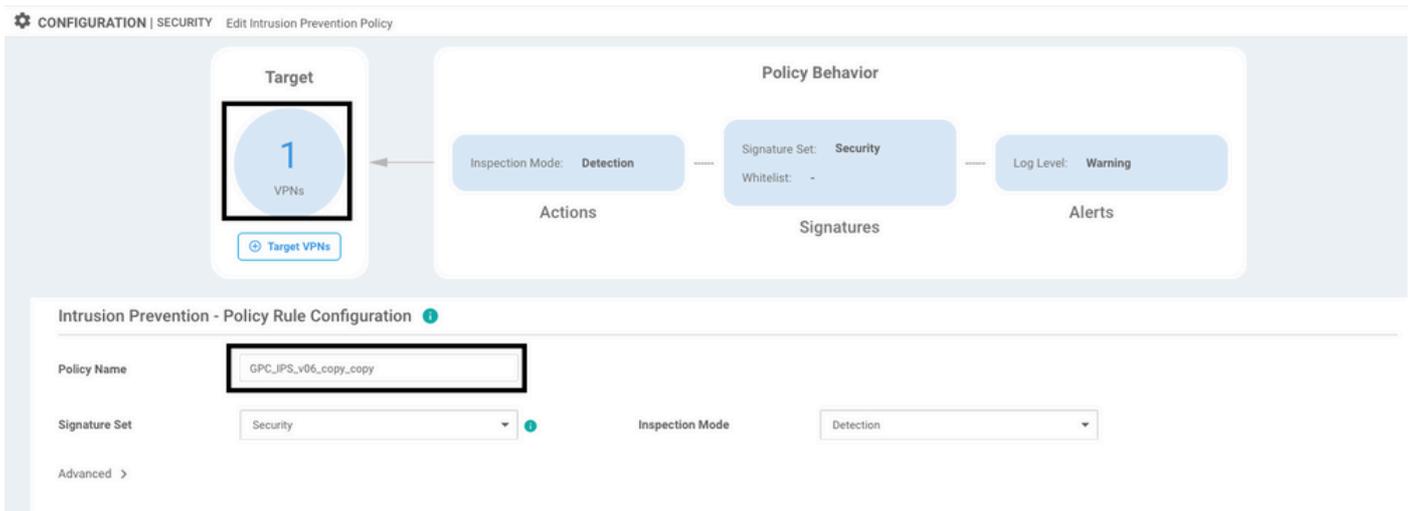
UTD 패키지가 필요한 IPS(Intrusion Prevention System), IDS(Intrusion Detection System), URL 필터링(URL-F), AMP(Advanced Malware Protection) 등의 보안 기능이 포함된 보안 정책을 사용하는

문제 3. 잘못된 참조

보안 정책 시퀀스에 대한 잘못된 참조를 방지하기 위해 보안 정책 기능에 사용되는 VPN/VRF가 cEdge 라우터에 이미 구성되어 있는지 확인합니다.



이 예에서 보안 정책에는 VPN/VRF 1에 대한 침입 방지 정책이 있지만 디바이스에는 구성된 VRF 1이 없습니다. 따라서 vmanage에서 해당 정책 시퀀스에 대한 잘못된 참조를 보냅니다.



보안 정책에서 언급한 VRF를 구성한 후에는 잘못된 참조가 나타나지 않으며 템플릿이 성공적으로 푸시됩니다.

문제 4. UTD가 설치되어 있고 활성화되어 있지만 활성화되지 않았습니다.

디바이스에 보안 정책이 구성되어 있고 UTD가 설치되어 있고 활성화되어 있지만 활성화되지 않았습니다.

이 문제는 문제 번호 3과 관련이 있습니다. 그러나 vManage에서는 컨피그레이션이 디바이스에 구성되지 않은 VRF를 참조하도록 허용했으며 정책이 어떤 VRF에도 적용되지 않았습니다.

라우터에 이 문제가 있는지 확인하려면 UTD가 활성 상태인지를 확인해야 합니다. UTD가 활성화되지 않음 메시지 및 정책이 VRF를 참조하지 않습니다.

```
Router01# show utd engine standard status
```


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.