# Installation des virtuellen UTD Security Images auf cEdge-Routern

## Inhalt



## Einleitung

In diesem Dokument wird die Installation von Unified Threat Defense (UTD) Security Virtual Image zur Aktivierung von Sicherheitsfunktionen auf Cisco IOS XE SD-WAN-Geräten beschrieben.

## Voraussetzungen

- Bevor Sie diese Funktionen nutzen, laden Sie das relevante virtuelle Sicherheits-Image in das vManage-Repository hoch.
- Der cEdge-Router muss sich im Verwaltungsmodus befinden und über eine Vorlage verfügen.
- Erstellen Sie eine Sicherheitsrichtlinienvorlage für Intrusion Prevention System (IPS), Intrusion Detection System (IDS), URL-Filterung (URL-F) oder Advanced Malware Protection (AMP)-Filterung.

### Anforderungen

- 4000 Integrated Services Router Cisco IOS XE SD-WAN (ISR4k)
- 1000 Integrated Services Router Cisco IOS XE SD-WAN (ISR1k)
- 1000v Cloud Services Router (CSR1kv)

- 1000v Integrated Services Router (ISRv)
- cEdges Plattformen, die 8 GB DRAM unterstützen.

## Verwendete Komponenten

- Virtuelles Cisco UTD-Image
- vManage-Controller
- cEdge Router mit Steuerungsanschlüssen mit Controllern.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

## Hintergrundinformationen

Für das Cisco UTD-Image muss eine Sicherheitsrichtlinie auf der Gerätevorlage installiert und Sicherheitsfunktionen wie Intrusion Prevention System (IPS), Intrusion Detection System (IDS), URL-Filterung (URL-F) und Advanced Malware Protection (AMP) auf Edge-Routern aktiviert werden.

Laden Sie die Software für die Cisco UTD Snort IP Engine von Cisco Software herunter.

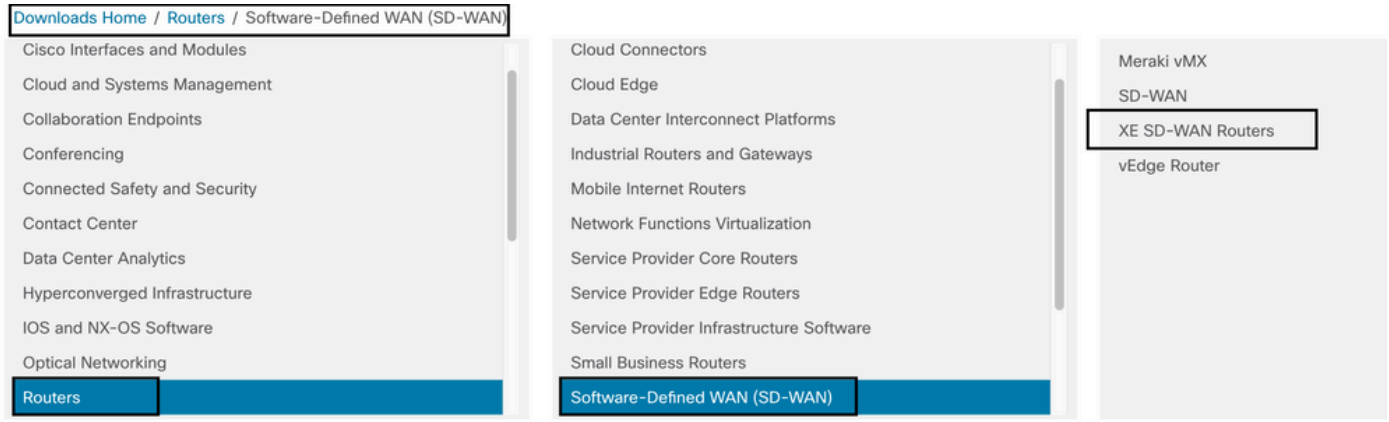
Verwenden Sie für die aktuelle Cisco IOS XE-Version den von Cisco UTD unterstützten regulären Ausdruck. Verwenden Sie den Befehl **show utd engine standard** version, um das empfohlene und unterstützte UTD-Image zu validieren.

```
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$
```

> **Hinweis** Der Pfad zum Herunterladen des Images hängt davon ab, ob auf dem Router die Cisco IOS XE SDWAN-Software (16.x) oder die Universal Cisco IOS XE-Software (17.x) ausgeführt wird.

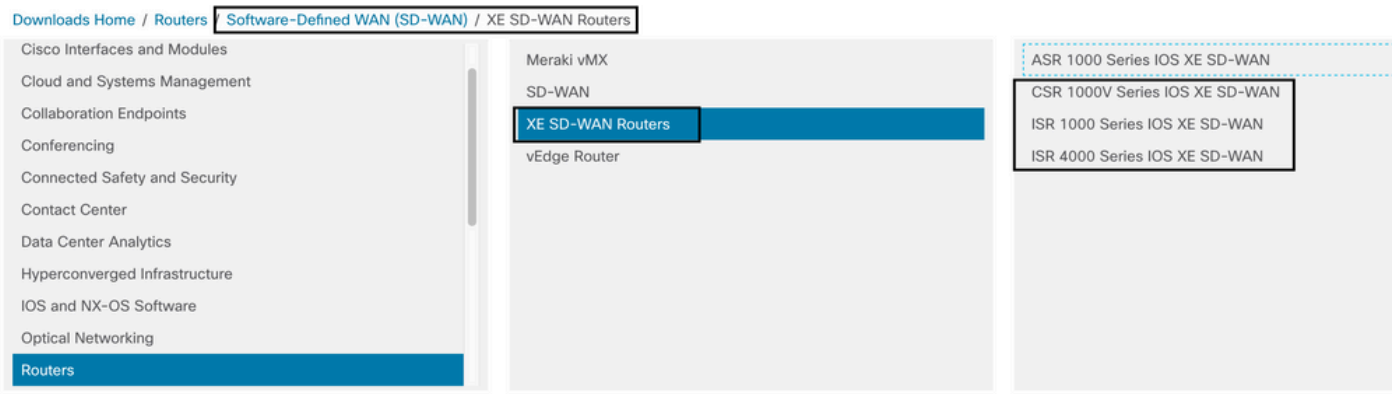
### Router mit Cisco IOS XE SDWAN-Software (16.x)

Die Software der Cisco UTD Snort IPS Engine steht für Router/Software-Defined WAN (SD-WAN)/XE SD-WAN-Router/ und den Integrated Router der Serie.




Wählen Sie den Modelltyp für den cEdge-Router aus.

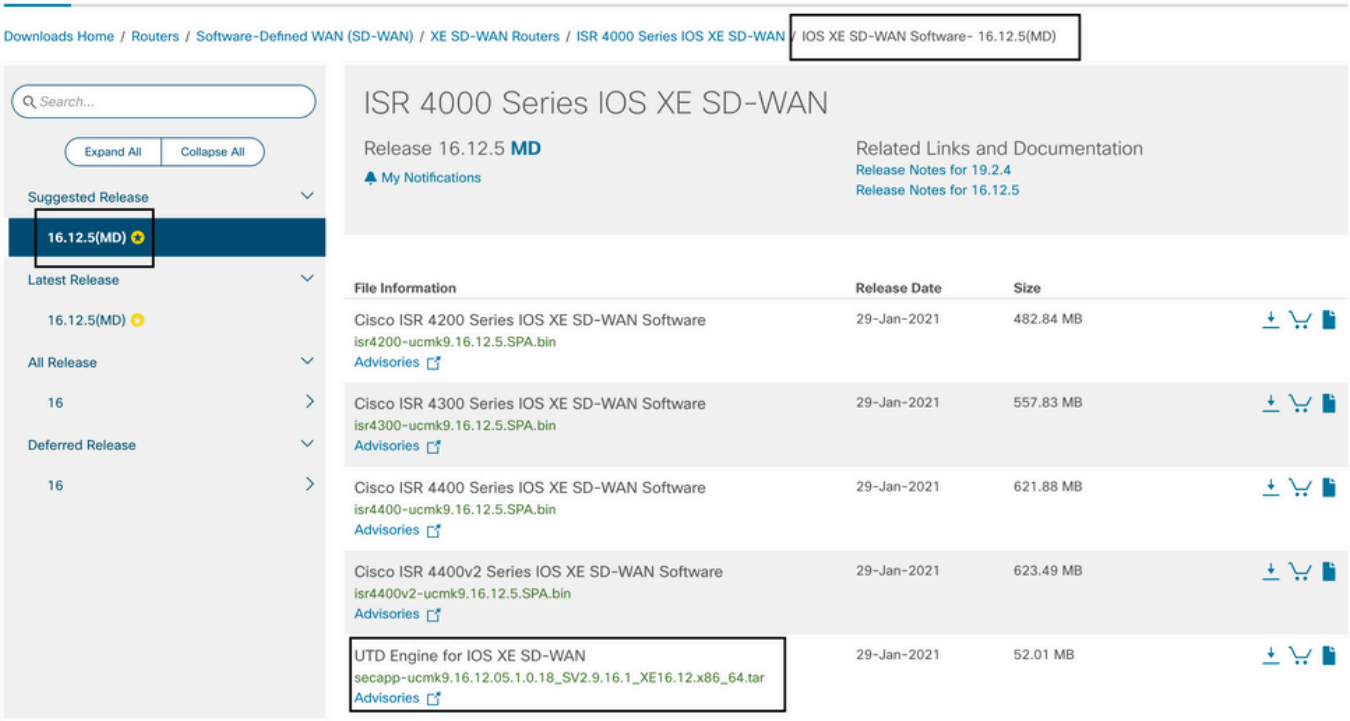
> **Hinweis** Aggregation Services Router (ASR) der Serie sind für UTD-Funktionen nicht verfügbar.




Nachdem Sie den Routertyp ausgewählt haben, wählen Sie die **Cisco IOS XE SD-WAN-**Softwareoption aus, um das UTD-Paket für Edges mit der Version 16.x zu erhalten.

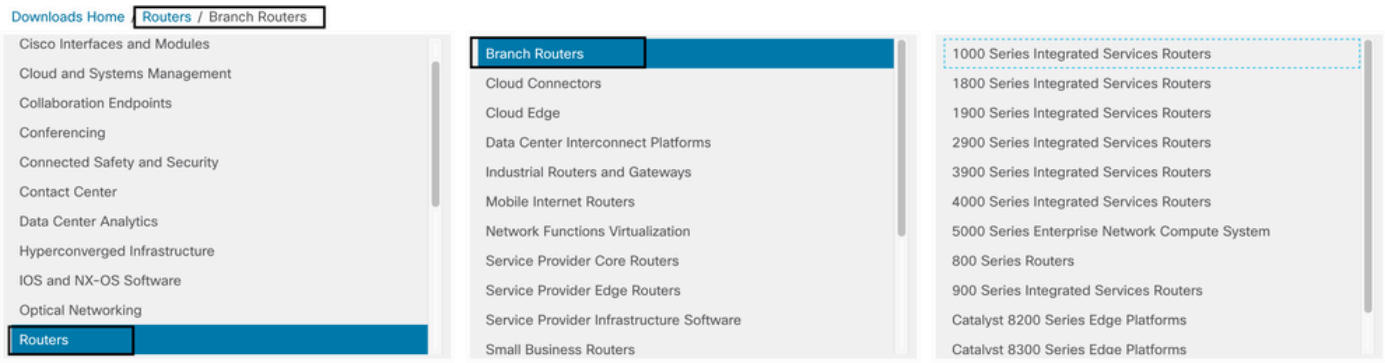

> **Hinweis** Der Downloadpfad zur Auswahl des virtuellen Cisco UTD-Images für den 16.x-Code für Edge-Router zeigt auch die **Cisco IOS XE-**Softwareoption an. Das ist der Pfad, um Upgrade-Codes von cEdge nur für 17.x zu wählen, aber es gibt nicht das virtuelle UTD-Image für Version 17.x. Cisco vereinheitlichte reguläre Cisco IOS XE- und Cisco IOS XE SDWAN-Codes für 17.x und neueste Versionen. Der Pfad zum virtuellen Cisco UTD-Image für 17.x entspricht dem regulären Cisco IOS XE-Code.

Wählen Sie die aktuelle Version des cEdge aus, und laden Sie das UTD-Paket für diese Version herunter.

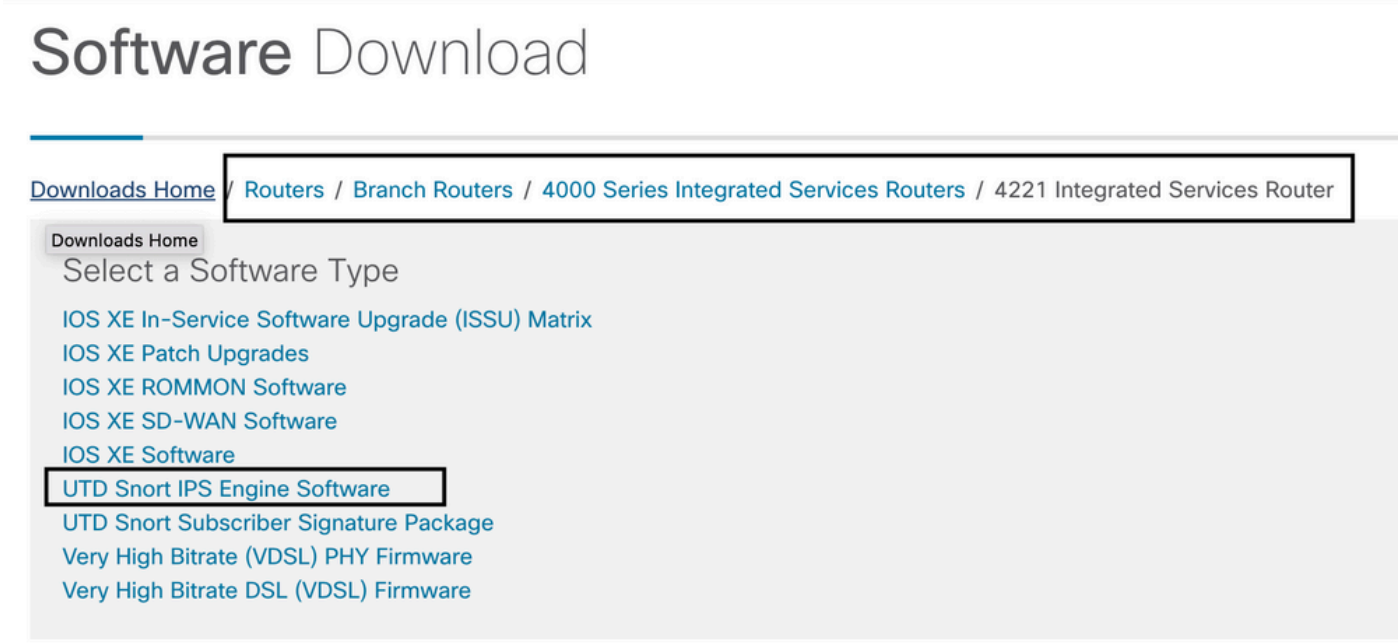



## Router mit Cisco IOS XE Software (17.x)

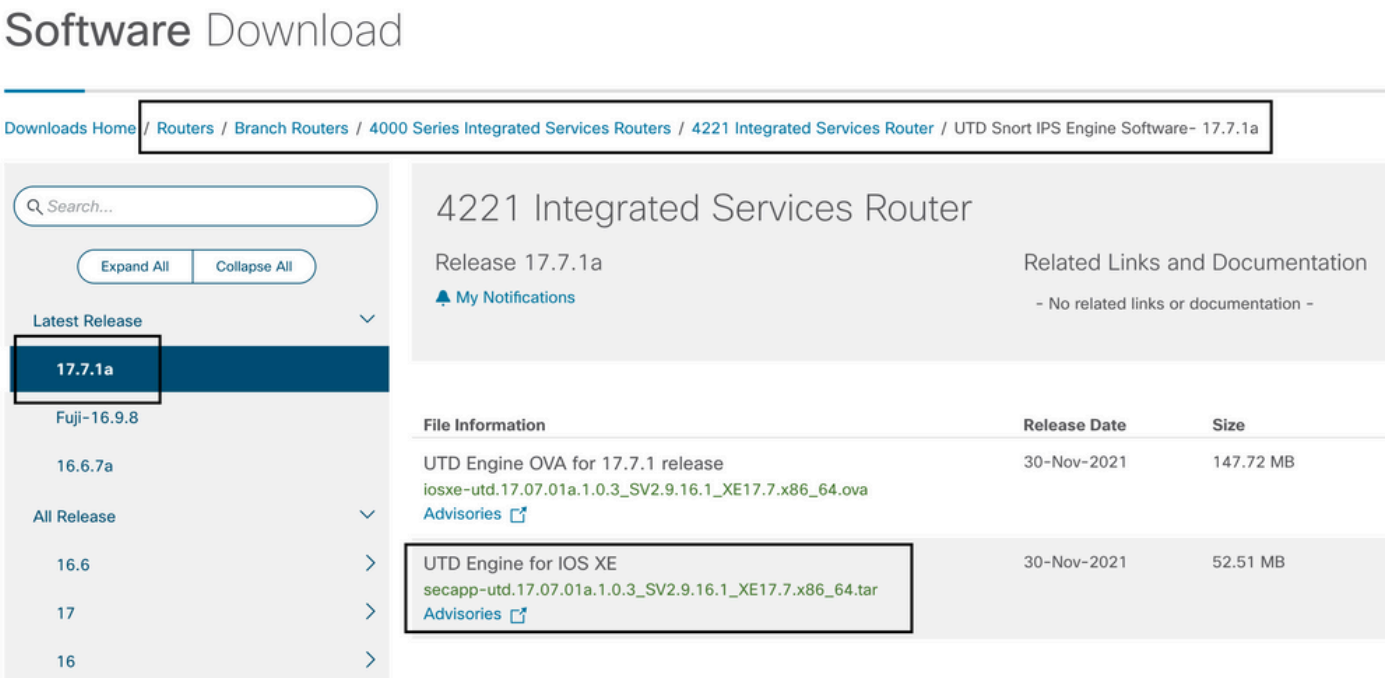
Cisco IOS XE Release 17.2.1r und die neueste Version verwenden das universalk9-Image für die Bereitstellung von Cisco IOS XE SD-WAN und Cisco IOS XE auf Cisco IOS XE-Geräten.
**Die UTD Snort IPS Engine-Software** befindet sich unter **Router > Zweigstellen-Router > Integrated Router der Serie**.




Nachdem Sie den Modelltyp des Routers ausgewählt haben, wählen Sie die **UTD Snort IPS Engine Software aus**.




Wählen Sie die aktuelle Version des Routers aus, und laden Sie das UTD-Paket für die ausgewählte Version herunter.

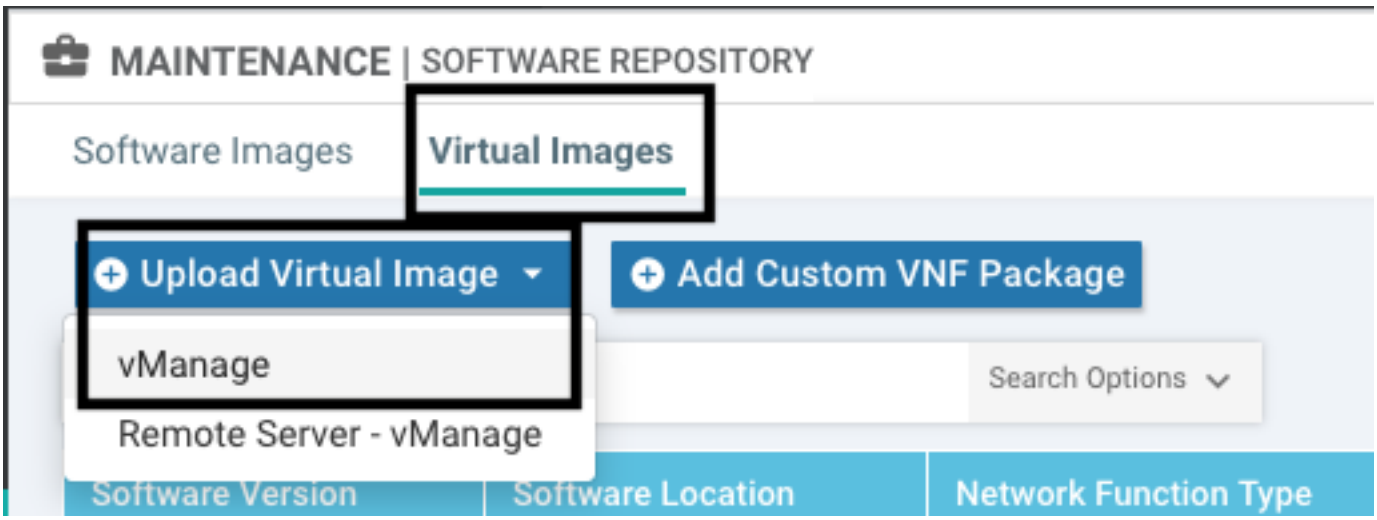


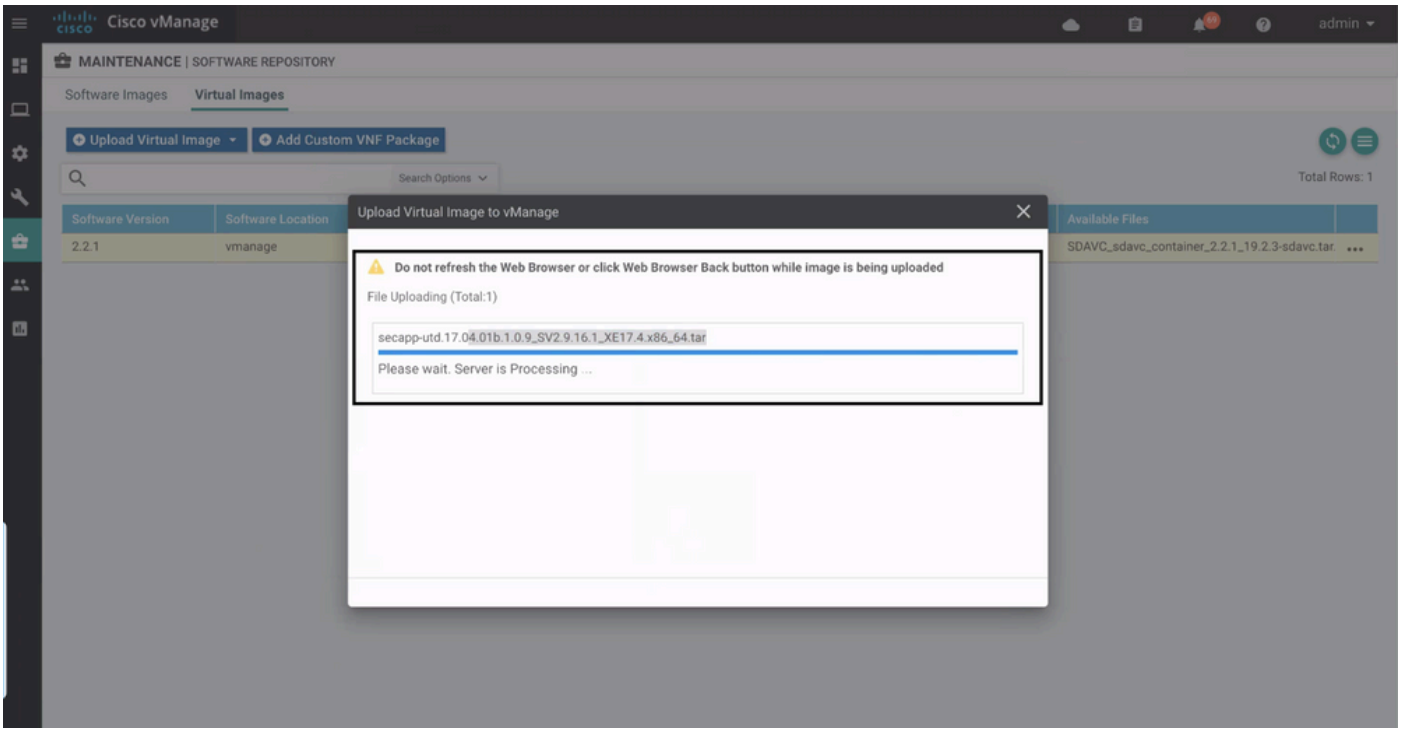

**Anmerkung:** Cisco Router der Serie ISR1100X (Cisco Nutella Router SR1100X-4G/6G) mit Cisco IOS XE Software anstelle von Viptela Code basieren auf x86_x64. Das für ISR4K veröffentlichte virtuelle Cisco UTD-Image kann darauf verwendet werden. Sie können dieselbe von Cisco UTD unterstützte Version des Bildcodes regex für die aktuelle Cisco IOS XE SDWAN-Version auf dem Nutella Router installieren. Verwenden Sie den Befehl **show utd engine standard version**, um das empfohlene und unterstützte Cisco UTD-Image für reguläre Ausdrücke zu validieren.

# Konfigurieren

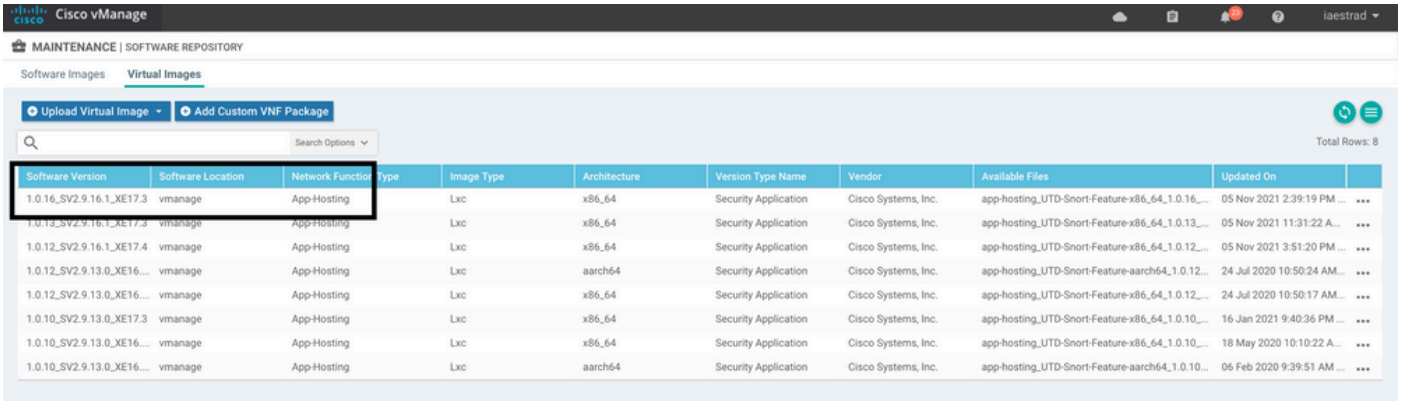
## Schritt 1: Virtuelles Image hochladen

Stellen Sie sicher, dass Ihr virtuelles Image mit dem aktuellen Cisco IOS XE SDWAN-Code auf dem cEdge übereinstimmt, und laden Sie es in das verwaltete Repository hoch.
Navigieren Sie zu **Maintenance > Software Repository > Virtual Image > Upload Virtual Image > vManage.**



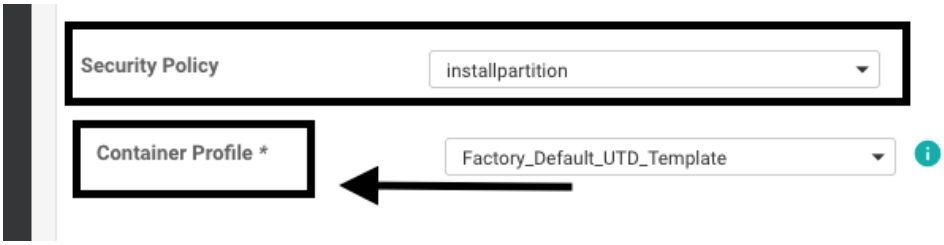




Nachdem das virtuelle Cisco UTD-Image erfolgreich hochgeladen wurde, überprüfen Sie erneut, ob es sich im Repository befindet.




## Schritt 2: Untervorlage "Sicherheitsrichtlinie und Containerprofil" zur Gerätevorlage hinzufügen

Fügen Sie der Gerätevorlage die zuvor erstellte Sicherheitsrichtlinie hinzu. Die Sicherheitsrichtlinie muss eine IPS/IDS-, URL-F- oder AMP-Filterrichtlinie für die Gerätevorlage enthalten. Öffnen Sie das Containerprofil automatisch. Verwenden Sie das Standardcontainerprofil, oder ändern Sie es bei Bedarf.

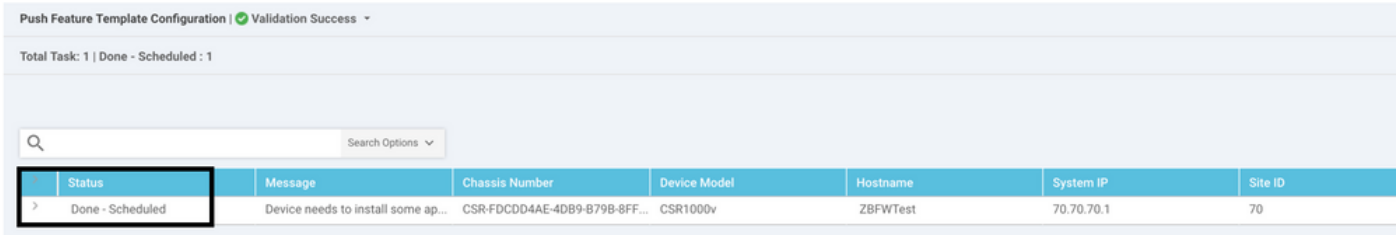



## Schritt 3: Aktualisieren oder Anhängen der Gerätevorlage mit dem Sicherheitsrichtlinien- und Containerprofil

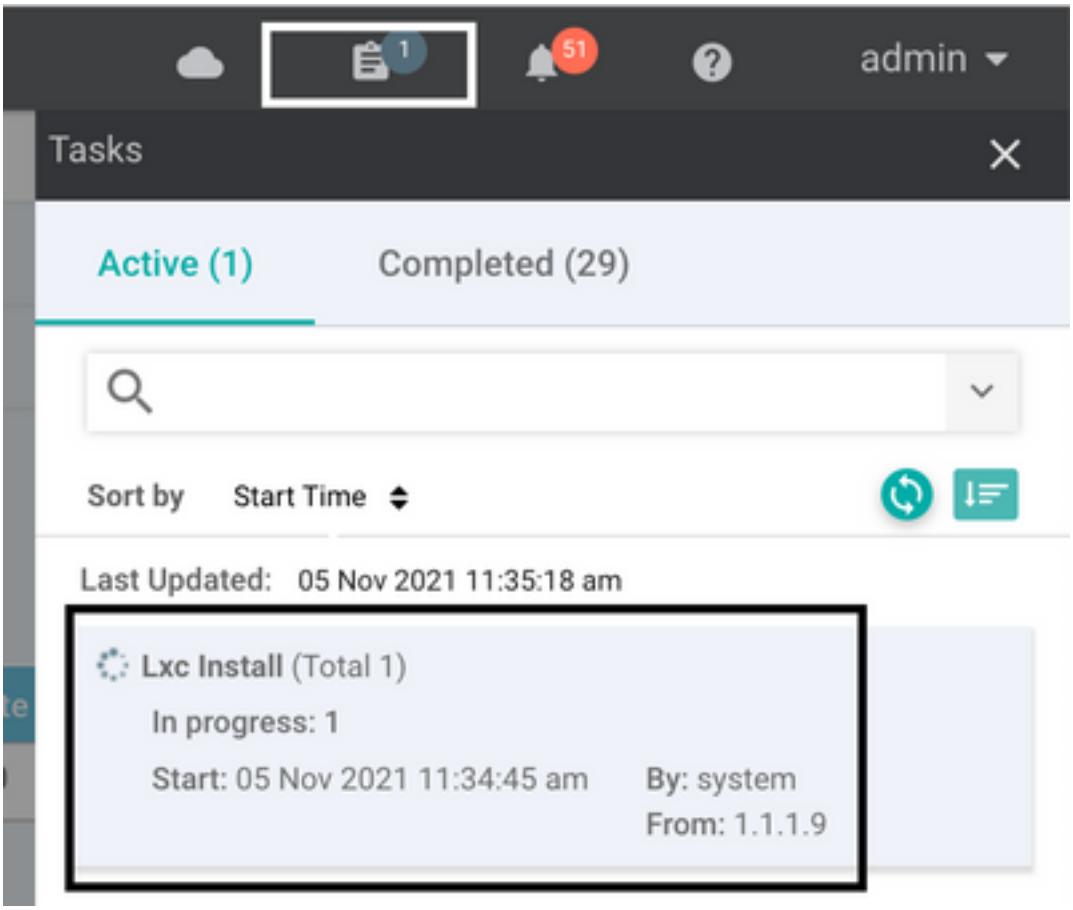
Aktualisieren Sie die Vorlage, oder fügen Sie sie an den cEdge-Router an. Beachten Sie bei Konfigurationsdiff, dass die App-Hosting-Konfiguration und die UTD-Engine für die Funktion IPS/IDS, URL-F oder AMP Filtering konfiguriert sind.

```
app-hosting appid utd
 app-resource package-profile cloud-low
 app-vnic gateway0 virtualportgroup 0 guest-interface 0
  guest-ipaddress 192.168.1.2 netmask 255.255.255.252
 !
 app-vnic gateway1 virtualportgroup 1 guest-interface 1
  guest-ipaddress 192.0.2.2 netmask 255.255.255.252
 !
 start
!
lldp run
nat64 translation timeout tcp 60
nat64 translation timeout udp 1
utd multi-tenancy
utd engine standard multi-tenancy
 threat-inspection profile GPC_IPS_v06_copy_copy
  threat detection
  policy security
  logging level warning
 !
 utd global
 !
!
policy
 no app-visibility
 no flow-visibility
 no implicit-acl-logging
 log-frequency        1000
!
```

Die Änderung des Vorlagenstatus in **Fertig geplant,** da der Manager bemerkte, dass die angewendete Konfiguration UTD-Modulfunktionen aufweist. Aus diesem Grund stellt vmanage fest, dass der cEdge das virtuelle Image installiert benötigt, um die UTD-Sicherheitsfunktionen verwenden zu können.




Nachdem die Vorlage in den Zeitplanstatus verschoben wurde, wird im Aufgabenmenü eine neue Aufgabe angezeigt, die **gerade ausgeführt wird.** Die neue Aufgabe ist die **LXC-Installation**. Dies bedeutet, dass der Manager die Installation des virtuellen Images auf dem cEdge automatisch startet, bevor die neue Konfiguration übertragen wird.

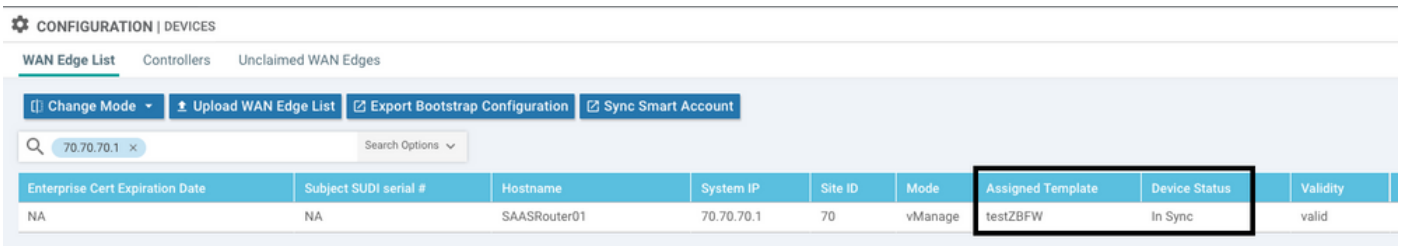



Sobald der LX-Container installiert ist, überträgt vManage die geplante Konfiguration mit den UTD-Funktionen. Hierfür ist keine neue Aufgabe vorhanden, da die Konfiguration bereits geplant war.


# Überprüfung

Überprüfen Sie, ob der cEdge mit vManage und angehängter Vorlage synchronisiert ist.

Navigieren Sie zu **Konfiguration > Geräte.**




Überprüfen Sie, ob die Cisco UTD-Version installiert ist:

```
Router02# show utd engine standard version
UTD Virtual-service Name: utd
IOS-XE Recommended UTD Version: 1.0.12_SV2.9.16.1_XE17.4
IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.4$
UTD Installed Version: 1.0.12_SV2.9.16.1_XE17.4         <<<<<<<<<<<<<<<<<<
```

**Hinweis: Die** installierte UTD-Version darf nicht den Status **UNSUPPORTED aufweisen**.

Überprüfen Sie, ob UTD mit der nächsten Ausgabe **ausgeführt** wird:

```
Router02# show app-hosting list
App id                                   State
---------------------------------------------------------
utd                                      RUNNING      <<<<<<<<<<<<<<<<<<
```

Der nächste Befehl fasst die vorherigen Befehle zusammen und zeigt den aktuellen Status und die aktuelle Version an:

```
Router02# show app-hosting detail appid utd
App id                 : utd
Owner                  : ioxm
State                  : RUNNING      <<<<<<<<<<<<<<<<<<<<<<<<
Application
  Type                 : LXC
  Name                 : UTD-Snort-Feature
  Version              : 1.0.12_SV2.9.16.1_XE17.4    <<<<<<<<<<<<<<<<<
  Description          : Unified Threat Defense
  Path                 : /bootflash/.UTD_IMAGES/iox-utd_1.0.12_SV2.9.16.1_XE17.4.tar
  URL Path             :
Activated profile name : cloud-low

Resource reservation
  Memory               : 2048 MB
  Disk                 : 861 MB
  CPU                  :
  CPU-percent          : 7 %
  VCPU                 : 0
```

**Der** Befehl **show utd engine standard status** zeigt den Zustand des UTD-Moduls an und listet die Uhrzeit auf, zu der das Signaturupdate abgerufen wird.

```
Router02# show utd engine standard status
Engine version       : 1.0.6_SV2.9.13.0_XE17.2
Profile              : Cloud-Low
System memory        :
              Usage  : 20.10 %
              Status : Green
Number of engines    : 1

Engine        Running    Health     Reason
=======================================
Engine(#1):   Yes        Green      None      <<<<<<<<<<<<<<<<<<<<<<<<<<<
=======================================================

Overall system status: Green    <<<<<<<<<<<<<<<<<<<<<<<<<

Signature update status:
========================
```

```
Current signature package version: 29130.156.s
Last update status: Successful
Last successful update time: Wed Nov 25 07:27:35 2020 EDT   <<<<<<<<<<<<<<<<<<<
Last failed update time: None
Last failed update reason: None
Next update scheduled at: None
Current status: Idle
```

Überprüfen Sie die aktivierten Funktionen mit dem nächsten Befehl:

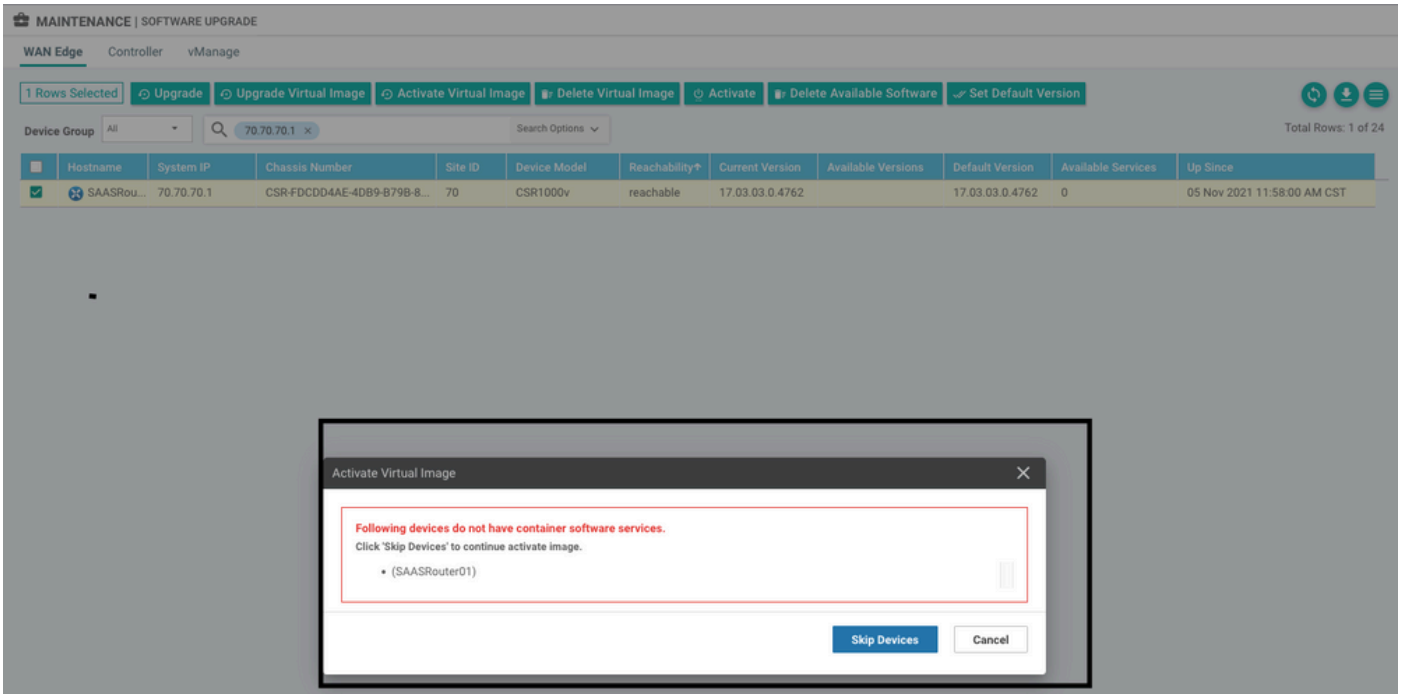
```
Router02# show platform hardware qfp active feature utd config
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: enabled
  Data plane initialized: yes
  TLS Decryption Policy: disabled
  Divert controller mode: enabled
  SN threads: 12
  CFT inst_id 0 feat id 2 fo id 2 chunk id 13
  Max flows: 55000
  SN Health: channel: Threat Defense : Green
  SN Health: channel: Service : Down

  Context Id: 0, Name: Global domain Security Context

   Ctx Flags: (0x1c70001)
        Engine: Standard
        State            : Enabled
        SN Redirect Mode : Fail-open, Divert
        Threat-inspection: Enabled, Mode: IPS
        Domain Filtering : Not Enabled
        URL Filtering    : Enabled   <<<<<<<<<<<
        File Inspection  : Enabled   <<<<<<<<<<<
        All Interfaces   : Enabled
```

# Häufige Probleme

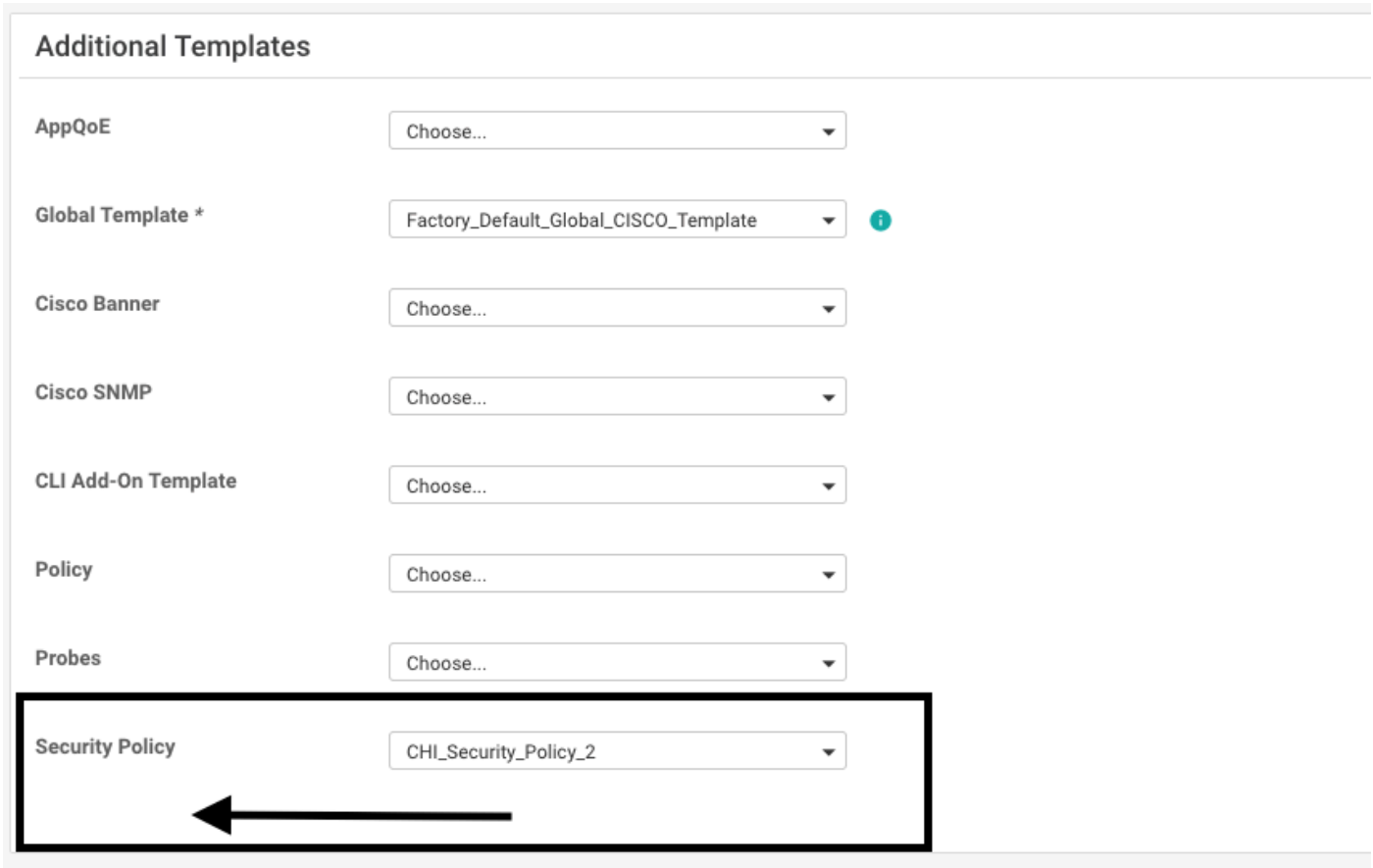
## AUFGABE 1. Fehler: Die folgenden Geräte verfügen nicht über Container-Software-Services

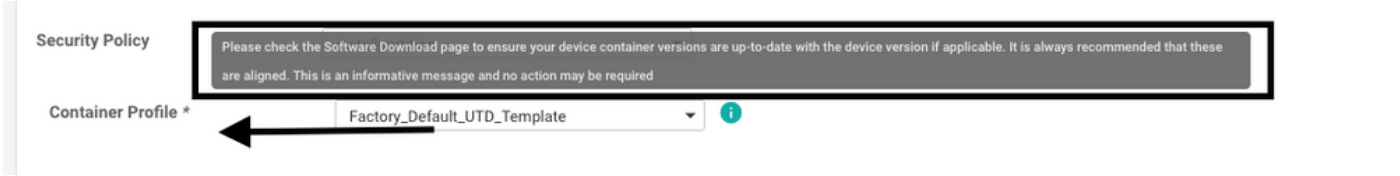
Aktivieren Sie das virtuelle Image.

Navigieren Sie zu **Wartung > Software > Aktivieren.**



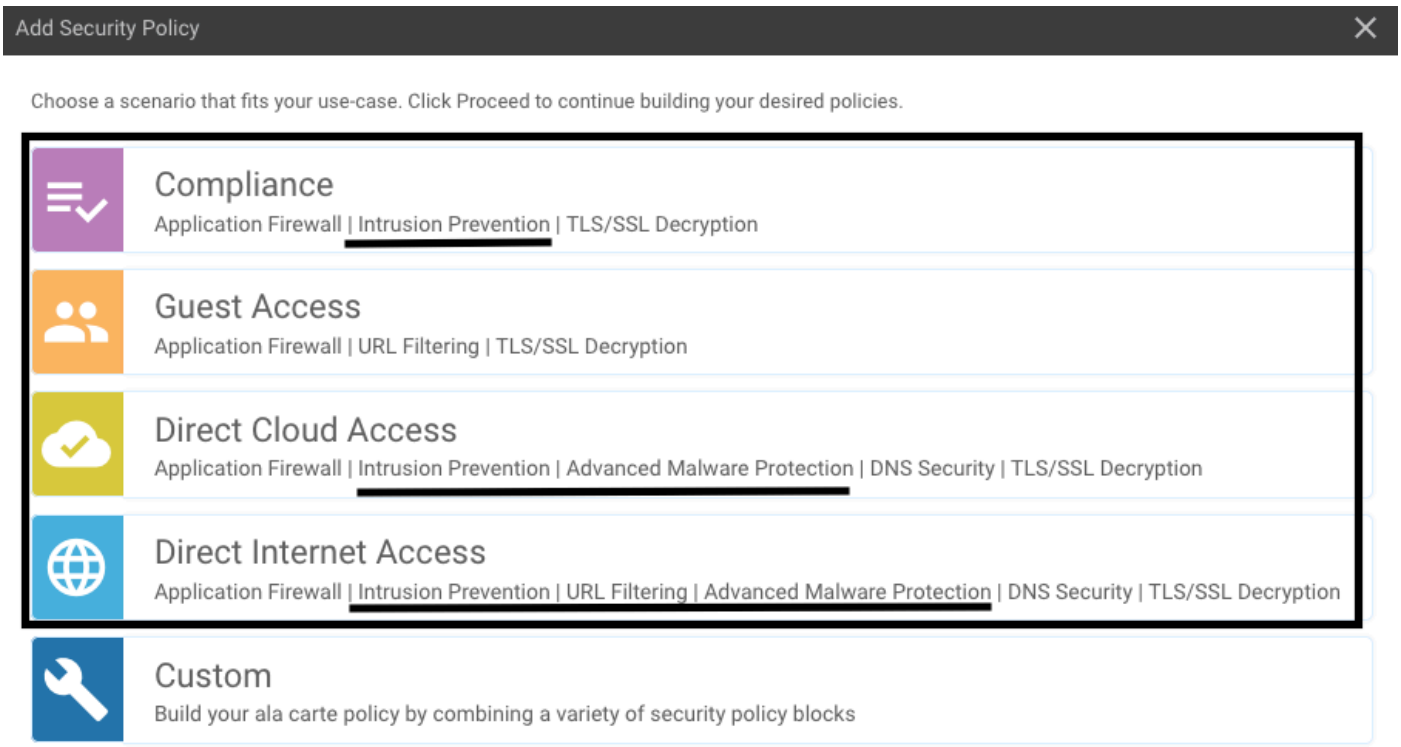

Das virtuelle Image sendet einen Fehler: **Geräte verfügen daher nicht über Container-Software-**Dienste. Wenn der ausgewählte cEdge-Router keine Sicherheitsrichtlinie mit der Containerprofil-Untervorlage besitzt.




Diese Vorlage wird automatisch hinzugefügt, wenn Sie eine Sicherheitsrichtlinie verwenden, die

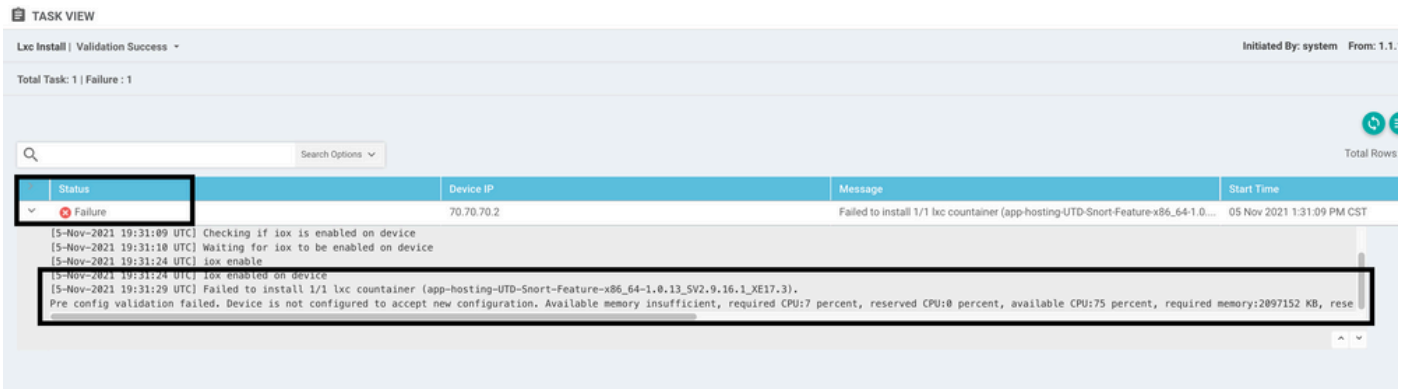
Sicherheitsfunktionen wie Intrusion Prevention System (IPS), Intrusion Detection System (IDS), URL-Filterung (URL-F) und Advanced Malware Protection (AMP) enthält, für die das UTD-Paket erforderlich ist. Nicht alle verfügbaren Sicherheitsfunktionen benötigen eine UTD-Engine wie die einfache ZBFW-Funktion.




Sobald Sie die Vorlage mit der Containerprofil-Untervorlage per Push übertragen haben, installiert der Manager automatisch das virtuelle Image.

## AUFGABE 2. Verfügbarer Speicher nicht ausreichend

Vergewissern Sie sich, dass der cEdge-Router über 8 GB DRAM-Speicher verfügt. Wenn dies nicht der Fall ist, **ist** der LXC-Installationsvorgang zum Senden eines **Geräts nicht so konfiguriert, dass es eine neue Konfiguration akzeptiert.** Fehler: **verfügbarer Speicher nicht ausreichend**. Für die Verwendung von UTD-Funktionen durch cEdge-Router sind mindestens 8 GB DRAM erforderlich.



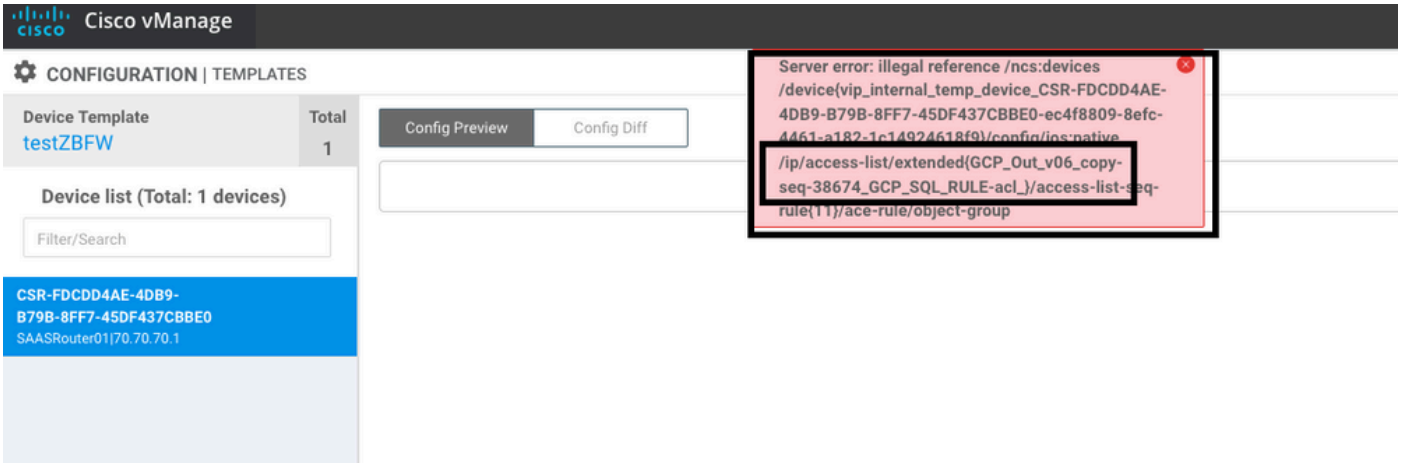

In diesem Fall verfügt der CSRv nur über 4 GB DRAM. Nach dem Upgrade des Speichers auf 8 GB DRAM ist die Installation erfolgreich.

Überprüfen Sie den aktuellen Gesamtspeicher mit **show sdwan system status** output:

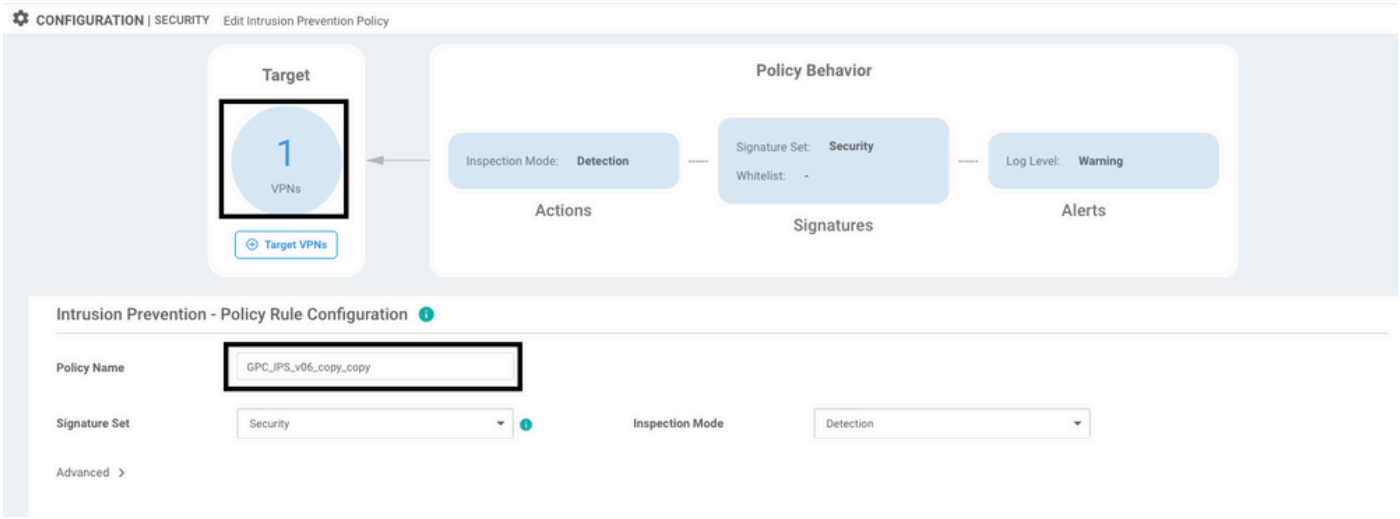
```
Router01# show sdwan system status

Memory usage:            8107024K total,    3598816K used,    4508208K free
                         349492K buffers,  2787420K cache
```

## AUSGABE 3. Rechtswidrige Bezugnahme

Vergewissern Sie sich, dass die VPNs/VRFs, die für die Sicherheitsrichtlinienfunktionen verwendet werden, bereits im cEdge-Router konfiguriert sind, um einen illegalen Verweis auf die Sicherheitsrichtliniensequenzen zu vermeiden.




In diesem Beispiel enthält die Sicherheitsrichtlinie eine Richtlinie zur Verhinderung von Eindringlingen für VPN/VRF 1, für die Geräte ist jedoch keine VRF 1 konfiguriert. Der Manager sendet eine illegale Referenz für diese Richtliniensequenz.




Nach der Konfiguration der in den Sicherheitsrichtlinien erwähnten VRF-Instanz wird der illegale Verweis nicht angezeigt, und die Vorlage wird erfolgreich übertragen.

## AUSGABE 4. UTD ist installiert und aktiv, aber nicht aktiviert.

Auf dem Gerät ist eine Sicherheitsrichtlinie konfiguriert, und UTD ist installiert und aktiv, aber nicht aktiviert.

Dieses Problem steht in Zusammenhang mit Problem Nr. 3. vManage hat jedoch zugelassen, dass die Konfiguration auf VRFs verweist, die nicht im Gerät konfiguriert sind, und die Richtlinie

wird nicht auf VRFs angewendet.

Um festzustellen, ob der Router mit diesem Problem konfrontiert ist, muss UTD aktiv sein. UTD-Nachricht nicht aktiviert, und die Richtlinie verweist nicht auf eine VRF-Instanz.

```
Router01# show utd engine standard status

UTD engine standard is not enabled <<<<<<<<<<<


ISR01#show sdwan virtual-application utd

VERSION                                 ACTIVE  PREVIOUS                      TIMESTAMP

-------------------------------------------------------------------------

1.0.16_SV2.9.16.1_XE17.3        true        true            2022-06-10T13:29:43-00:00
```

Überprüfen Sie die Ziel-VPNs, und wenden Sie die Richtlinie auf eine konfigurierte VRF-Instanz an.

# Zugehörige Informationen

- Router-Sicherheit: Snort IPS auf Routern
- Cisco SD-WAN Security Configuration Guide, Cisco IOS XE Version
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.