

Installeer UTD Security Virtual Image op cEdge-routers

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Routers waarop Cisco IOS XE SDWAN-software \(16.x\) wordt uitgevoerd](#)

[Routers waarop Cisco IOS XE-software \(17.x\) wordt uitgevoerd](#)

[Configureren](#)

[Stap 1. Virtuele afbeelding uploaden](#)

[Stap 2. Voeg beveiligingsbeleid en subsjabloon voor containerprofiel toe aan apparaatsjabloon](#)

[Stap 3. Werk de apparaatsjabloon bij of voeg deze toe met het beveiligingsbeleid en het containerprofiel](#)

[Verifiëren](#)

[Veelvoorkomende problemen](#)

[PROBLEEM 1. Fout: Volgende Apparaten hebben geen Container Software Services](#)

[PROBLEEM 2. ONVOLDOENDE BESCHIKBAAR GEHEUGEN](#)

[Probleem 3. Onrechtmatige verwijzing](#)

[Probleem 4. UTD is geïnstalleerd en actief maar niet ingeschakeld](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u een virtuele image van Unified Threat Defense (UTD) installeert om beveiligingsfuncties in te schakelen op Cisco IOS XE SD-WAN-apparaten.

Voorwaarden

- Voordat u deze functies gebruikt, kunt u de relevante Security Virtual Image uploaden naar de vManager-opslagplaats.
- cEdge-router moet in de beheermodus staan, met sjabloon vooraf als bijlage.
- Maak een Security Policy Template voor Inbraakpreventiesysteem (IPS), Inbraakdetectiesysteem (IDS), URL-filtering (URL-F) of Advanced Malware Protection (AMP) filtering.

Vereisten

- 4000 geïntegreerde services router Cisco IOS XE SD-WAN (ISR4k)
- 1000 geïntegreerde services router Cisco IOS XE SD-WAN (ISR1k)
- 1000v router voor cloudservices (CSR1kv),

- 1000v geïntegreerde services router (ISRV)
- Randplatforms die 8GB DRAM ondersteunen.

Gebruikte componenten

- Cisco UTD virtuele image
- vManager-controller
- cEdge-routers met controleverbindingen met controllers.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Cisco UTD-afbeelding heeft een beveiligingsbeleid nodig met betrekking tot de te installeren apparaatsjabloon, en inbraakpreventiesysteem (IPS), inbraakdetectiesysteem (IDS), URL-filtering (URL-F) en Advanced Malware Protection (AMP) op routers.

De software voor Cisco UTD Snort IP Engine downloaden van [Software van Cisco](#)

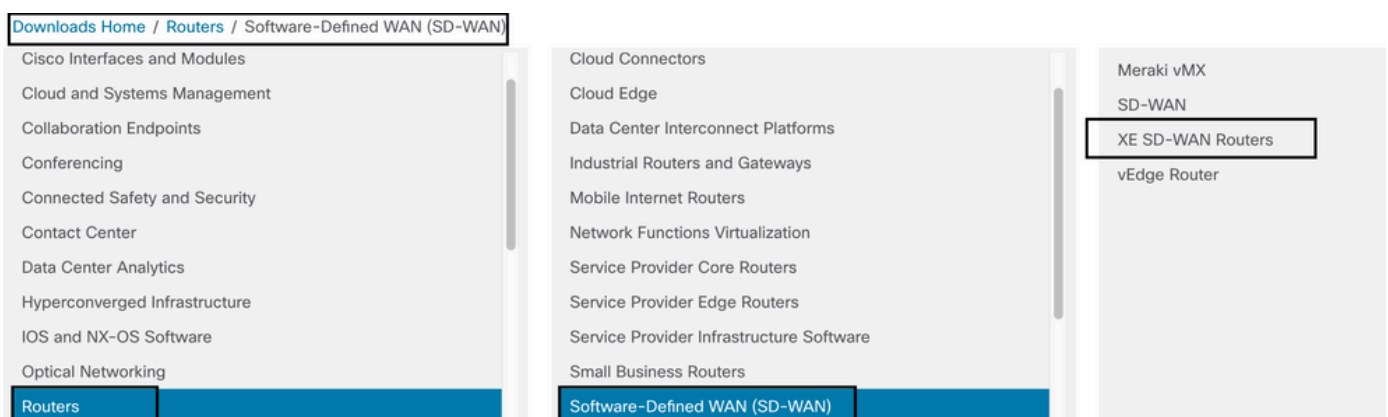
Gebruik het door Cisco UTD virtuele image ondersteunde programma Regex voor de huidige Cisco IOS XE-versie. Gebruik de opdracht **tonen utd motor standaard** versie om de aanbevolen en ondersteunde UTD-afbeelding te valideren.

```
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$
```

Opmerking Het pad om de afbeelding te downloaden hangt af van de vraag of de router Cisco IOS XE SDWAN-software (16.x) of Universal Cisco IOS XE-software (17.x) gebruikt.

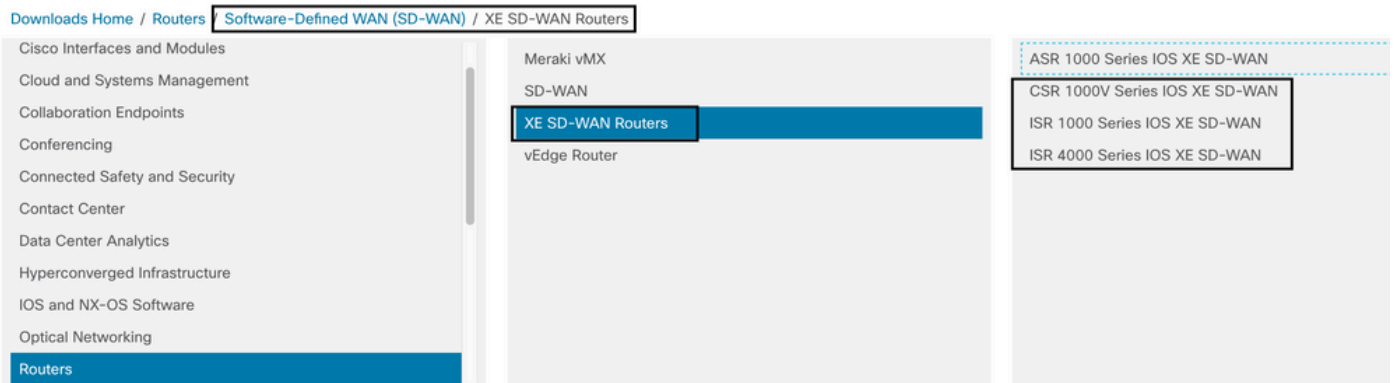
Routers waarop Cisco IOS XE SDWAN-software (16.x) wordt uitgevoerd

Het pad om de Cisco UTD Snel IPS Engine software te krijgen is Routers/ Software-Defined WAN (SD-WAN)/ XE SD-WAN routers / en de Series geïntegreerde router.



Kies het modeltype voor de cEdge-router.

Opmerking: Series Aggregation Services Routers (ASR) zijn niet beschikbaar voor UTD-functies.



Nadat u het type router model kiest, selecteer de **Cisco IOS XE SD-WAN software** optie om het UTD pakket voor cEdge op 16.x versie te krijgen.

Downloads Home / Routers / Software-Defined WAN (SD-WAN) / XE SD-WAN Routers / ISR 4000 Series IOS XE SD-WAN

Select a Software Type

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

[IOS XE SD-WAN Software](#)

[IOS XE Software](#)

Opmerking Het downloadpad om de virtuele Cisco UTD-afbeelding voor 16.x-code voor cEdge-routers te kiezen, toont ook **Cisco IOS XE**-softwareoptie. Dat is het pad om upgradecodes van cEdge alleen voor 17.x te kiezen, maar er is niet gevonden het UTD virtuele beeld voor versie 17.x. Cisco Unified regular Cisco IOS XE en Cisco IOS XE SDWAN-codes op 17.x en hoger, zodat het pad om de Cisco UTD virtuele afbeelding voor 17.x te verkrijgen, hetzelfde is als de reguliere Cisco IOS XE-codes.

Kies de huidige versie van de cEdge en download het UTD-pakket voor die versie.

Search...

Expand All Collapse All

Suggested Release

16.12.5(MD)

Latest Release

16.12.5(MD)

All Release

16

Deferred Release

16

ISR 4000 Series IOS XE SD-WAN

Release 16.12.5 **MD**

[My Notifications](#)

Related Links and Documentation

[Release Notes for 19.2.4](#)

[Release Notes for 16.12.5](#)

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	↓ 🛒 📄

Routers waarop Cisco IOS XE-software (17.x) wordt uitgevoerd

Cisco IOS XE release 17.2.1r en het nieuwste gebruik van het universalk9-image om zowel Cisco IOS XE SD-WAN als Cisco IOS XE op Cisco IOS XE-apparaten te implementeren.

UTD Snort IPS Engine software bevindt zich in **Routers > Branch Routers > Series geïntegreerde router**.

Downloads Home **Routers / Branch Routers**

- Cisco Interfaces and Modules
- Cloud and Systems Management
- Collaboration Endpoints
- Conferencing
- Connected Safety and Security
- Contact Center
- Data Center Analytics
- Hyperconverged Infrastructure
- IOS and NX-OS Software
- Optical Networking
- Routers**

Branch Routers

- Cloud Connectors
- Cloud Edge
- Data Center Interconnect Platforms
- Industrial Routers and Gateways
- Mobile Internet Routers
- Network Functions Virtualization
- Service Provider Core Routers
- Service Provider Edge Routers
- Service Provider Infrastructure Software
- Small Business Routers

- 1000 Series Integrated Services Routers**
- 1800 Series Integrated Services Routers
- 1900 Series Integrated Services Routers
- 2900 Series Integrated Services Routers
- 3900 Series Integrated Services Routers
- 4000 Series Integrated Services Routers
- 5000 Series Enterprise Network Compute System
- 800 Series Routers
- 900 Series Integrated Services Routers
- Catalyst 8200 Series Edge Platforms
- Catalyst 8300 Series Edge Platforms

Nadat u het modeltype van de router hebt gekozen, selecteert u de **UTD Snel IPS Engine Software**.

Software Download

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

Downloads Home

Select a Software Type

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

[IOS XE Patch Upgrades](#)

[IOS XE ROMMON Software](#)

[IOS XE SD-WAN Software](#)

[IOS XE Software](#)

[UTD Snort IPS Engine Software](#)

[UTD Snort Subscriber Signature Package](#)

[Very High Bitrate \(VDSL\) PHY Firmware](#)

[Very High Bitrate DSL \(VDSL\) Firmware](#)

Selecteer de huidige versie van de router en download het UTD-pakket voor de geselecteerde versie.

Software Download

[Downloads Home](#) / [Routers](#) / [Branch Routers](#) / [4000 Series Integrated Services Routers](#) / [4221 Integrated Services Router](#) / [UTD Snort IPS Engine Software- 17.7.1a](#)

[Expand All](#) [Collapse All](#)

Latest Release

- 17.7.1a**
- Fuji-16.9.8
- 16.6.7a

All Release

- 16.6
- 17
- 16

4221 Integrated Services Router

Release 17.7.1a

[My Notifications](#)

Related Links and Documentation
- No related links or documentation -

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

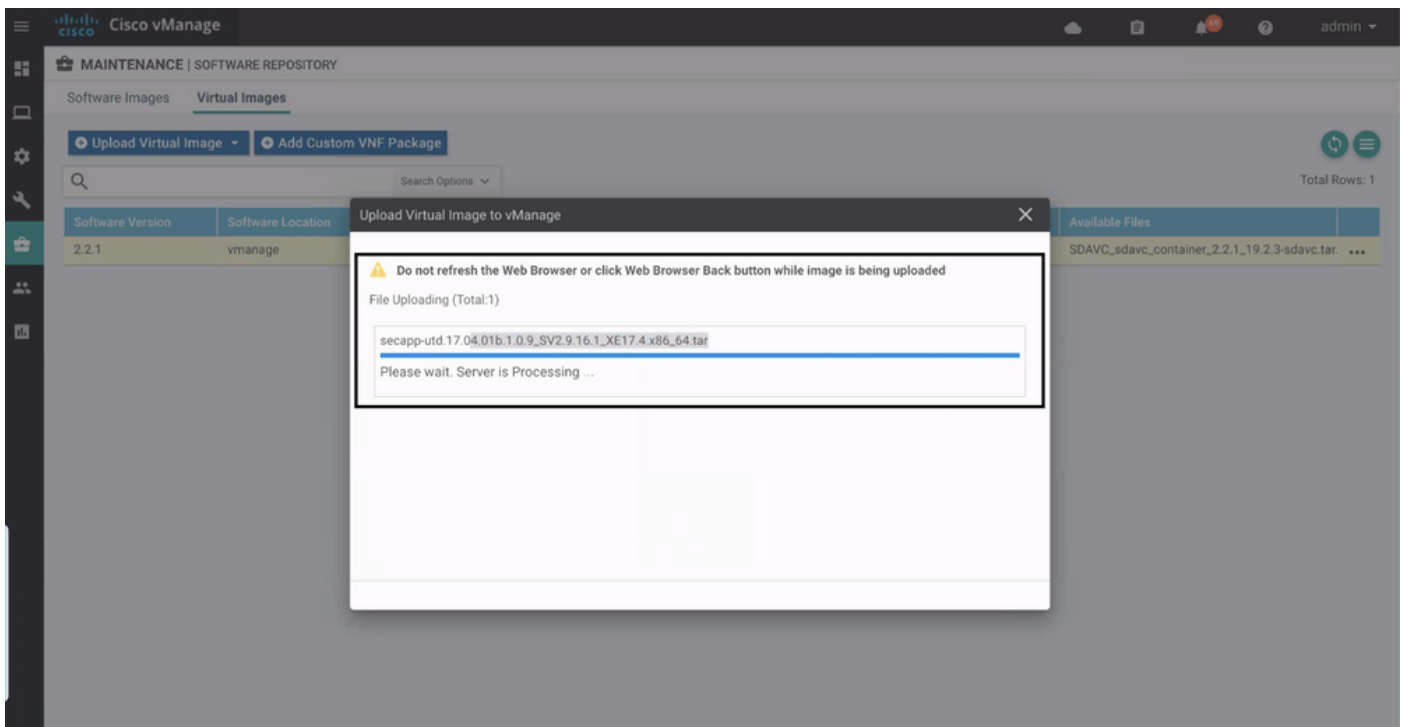
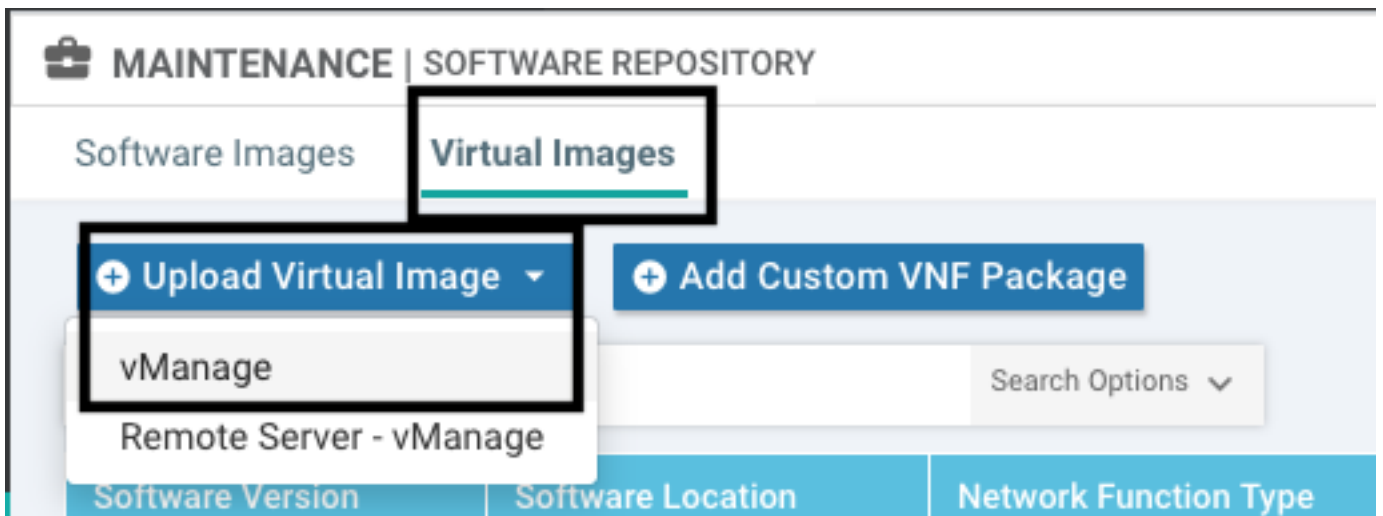
Opmerking: Cisco ISR1100X Series-routers (Cisco Nutella Routers SR1100X-4G/6G) die Cisco IOS XE-software uitvoeren in plaats van Viptela-code zijn gebaseerd op x86_x64. Het virtuele beeld dat Cisco UTD publiceert voor ISR4K kan eraan werken. U kunt dezelfde versie van Cisco UTD-beeldcode installeren die wordt ondersteund door Regex voor de huidige Cisco IOS XE SDWAN-versie op de Nutella-router. Gebruik de opdracht **tonen utd motor standaard versie** om de aanbevolen en ondersteunde regex Cisco UTD-afbeelding te valideren.

Configureren

Stap 1. Virtuele afbeelding uploaden

Zorg ervoor dat uw virtuele afbeelding overeenkomt met de huidige Cisco IOS XE SDWAN-code op de cEdge en upload deze naar de opslagplaats.

Ga naar **Onderhoud > Software Repository > Virtual Image > Upload Virtual Image > vManager**.



Zodra de virtuele afbeelding van Cisco UTD succesvol is geüpload, controleert u of deze zich in de repository bevindt.



Cisco vManage MAINTENANCE | SOFTWARE REPOSITORY

Software Images Virtual Images

Upload Virtual Image Add Custom VNF Package

Search Options

Total Rows: 8

Software Version	Software Location	Network Function	Type	Image Type	Architecture	Version Type Name	Vendor	Available Files	Updated On
1.0.16_SV2.9.16.1_XE17.3	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.16...	05 Nov 2021 2:39:19 PM ...
1.0.13_SV2.9.16.1_XE17.2	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.13...	05 Nov 2021 11:31:22 A ...
1.0.12_SV2.9.16.1_XE17.4	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.12...	05 Nov 2021 3:51:20 PM ...
1.0.12_SV2.9.13.0_XE16...	vmanage	App-Hosting	Lxc	aarch64	aarch64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-aarch64_1.0.12...	24 Jul 2020 10:50:24 AM...
1.0.12_SV2.9.13.0_XE16...	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.12...	24 Jul 2020 10:50:17 AM...
1.0.10_SV2.9.13.0_XE17.3	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.10...	16 Jan 2021 9:40:36 PM ...
1.0.10_SV2.9.13.0_XE16...	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.10...	18 May 2020 10:10:22 A ...
1.0.10_SV2.9.13.0_XE16...	vmanage	App-Hosting	Lxc	aarch64	aarch64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-aarch64_1.0.10...	06 Feb 2020 9:39:51 AM ...

Stap 2. Voeg beveiligingsbeleid en subsjabloon voor containerprofiel toe aan apparaatsjabloon

Voeg het eerder gemaakte beveiligingsbeleid toe aan de apparaatsjabloon. Het beveiligingsbeleid moet een IPS/IDS-, URL-F- of AMP-filteringsbeleid hebben om de apparaatsjabloon aan te passen. Open het containerprofiel automatisch. Gebruik het standaardcontainerprofiel of wijzig het indien nodig.

The image shows two configuration fields. The first field is labeled "Security Policy" and has a dropdown menu with "installpartition" selected. The second field is labeled "Container Profile *" and has a dropdown menu with "Factory_Default_UTD_Template" selected. An arrow points from the "Container Profile" field to the left.

Stap 3. Werk de apparaatsjabloon bij of voeg deze toe met het beveiligingsbeleid en het containerprofiel

Werk de sjabloon bij of voeg deze toe aan de cEdge-router. Opmerking over het configuratieverschil dat de configuratie van de app en de UTD-engine voor de functie IPS/IDS, URL-F of AMP-filtering zijn geconfigureerd.

```

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
272 utd multi-tenancy
273 utd engine standard multi-tenancy
274   threat-inspection profile GPC_IPS_v06_copy_copy
275   threat detection
276   policy security
277   logging level warning
278 !
279 utd global
280 !
281 !
282 policy
283   no app-visibility
284   no flow-visibility
285   no implicit-acl-logging
286   log-frequency 1000
287 !

```

Sjabloonstatus wijzigen in **Klaar-gepland** omdat vManager opmerkte dat de toegepaste configuratie UTD-motorfuncties heeft, dus vManager bepalen dat de cEdge de virtuele afbeelding nodig heeft die is geïnstalleerd om de UTD-beveiligingsfuncties te gebruiken.

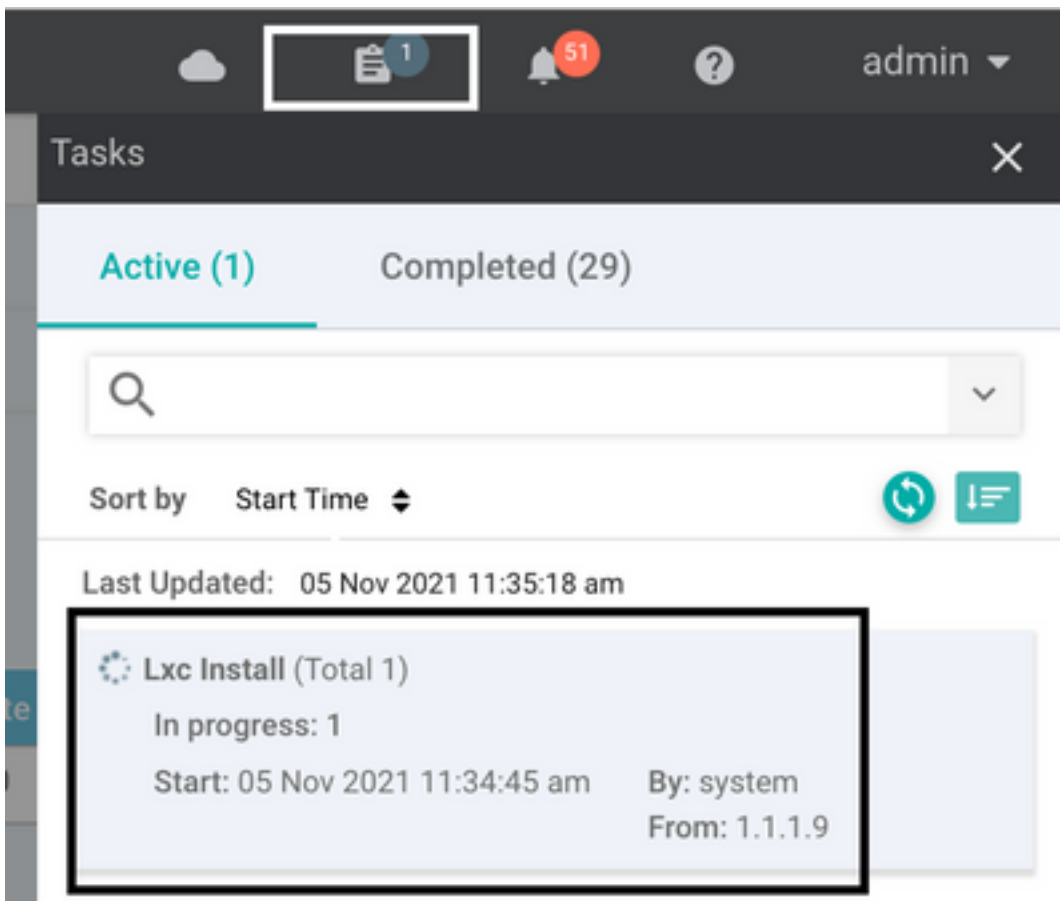
Push Feature Template Configuration | Validation Success

Total Task: 1 | Done - Scheduled : 1

Search Options

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

Nadat de sjabloon naar de planningsstatus is verplaatst, wordt een nieuwe taak in **uitvoering** weergegeven in het taakmenu. De nieuwe taak is de **LXC-installatie**, wat betekent dat de beheerder automatisch de installatie van het virtuele beeld naar de cEdge start voordat de nieuwe configuratie wordt geduwd.



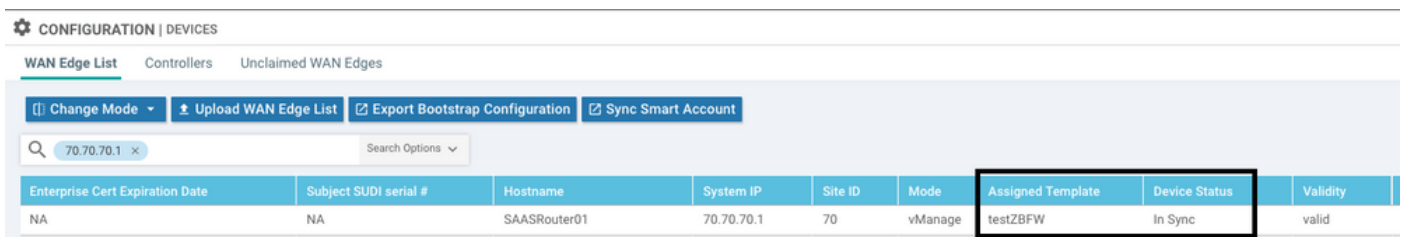
Nadat de LX-container is geïnstalleerd, drukt vManager de configuratie vooraf met de UTD-functies. Er is geen nieuwe taak hiervoor omdat de configuratie eerder was gepland.



Verifiëren

Controleer of de cEdge synchron is met vManager en de bijbehorende sjabloon.

Navigeren naar **configuratie > Apparaten**



Controleer of de Cisco UTD-versie is geïnstalleerd:

MAINTENANCE | SOFTWARE UPGRADE

WAN Edge Controller vManage

1 Rows Selected Upgrade Upgrade Virtual Image Activate Virtual Image Delete Virtual Image Activate Delete Available Software Set Default Version

Device Group All 70.70.70.1 Search Options Total Rows: 1 of 24

Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability*	Current Version	Available Versions	Default Version	Available Services	Up Since
SAASRou...	70.70.70.1	CSR-FDCDD4AE-4DB9-B798-8...	70	CSR1000v	reachable	17.03.03.0.4762		17.03.03.0.4762	0	05 Nov 2021 11:58:00 AM CST

Activate Virtual Image

Following devices do not have container software services.
Click 'Skip Devices' to continue activate image.

- (SAASRouter01)

Skip Devices Cancel

Het virtuele beeld verstuurt een fout: **Apparaten hebben dus geen containersoftware**, Als de geselecteerde cEdge-router geen beveiligingsbeleid heeft met het containerprofiel-sjabloon.

Additional Templates

AppQoE Choose...

Global Template * Factory_Default_Global_CISCO_Template ⓘ

Cisco Banner Choose...

Cisco SNMP Choose...

CLI Add-On Template Choose...

Policy Choose...

Probes Choose...

Security Policy CHI_Security_Policy_2

Security Policy

Please check the Software Download page to ensure your device container versions are up-to-date with the device version if applicable. It is always recommended that these are aligned. This is an informative message and no action may be required

Container Profile * Factory_Default_UTD_Template ⓘ

Deze sjabloon wordt automatisch toegevoegd als u een beveiligingsbeleid gebruikt dat beveiligingsfuncties bevat zoals Inbraakpreventiesysteem (IPS), Inbraakdetectiesysteem (IDS),

URL-filtering (URL-F) en Advanced Malware Protection (AMP) waarvoor UTD-pakket nodig is. Niet alle beveiligingsfuncties die beschikbaar zijn, hebben UTD-engine nodig, zoals eenvoudige ZBFW-functie.

Add Security Policy [X]

Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

- Compliance**
Application Firewall | Intrusion Prevention | TLS/SSL Decryption
- Guest Access**
Application Firewall | URL Filtering | TLS/SSL Decryption
- Direct Cloud Access**
Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security | TLS/SSL Decryption
- Direct Internet Access**
Application Firewall | Intrusion Prevention | URL Filtering | Advanced Malware Protection | DNS Security | TLS/SSL Decryption
- Custom**
Build your ala carte policy by combining a variety of security policy blocks

Zodra u de sjabloon met de subsjabloon van het containerprofiel duwt, installeert de beheerder automatisch de virtuele afbeelding.

PROBLEEM 2. ONVOLDOENDE BESCHIKBAAR GEHEUGEN

Zorg ervoor dat de cEdge router 8 GB DRAM geheugen heeft, als dat niet het geval is, het Lxc Installatie proces verzenden een apparaat is niet geconfigureerd om nieuwe configuratie te accepteren. Beschikbaar geheugen onvoldoende fout. De vereisten voor cEdge-routers om UTD-functies te gebruiken, zijn minimaal 8 GB aan DRAM's.

TASK VIEW

Lxc Install | Validation Success - [Initiated By: system From: 1.1.]

Total Task: 1 | Failure: 1

Status	Device IP	Message	Start Time
Failure	70.70.70.2	Failed to install 1/1 lxc container (app-hosting-UTD-Snort-Feature-x86_64-1.0...)	05 Nov 2021 1:31:09 PM CST

```
[5-Nov-2021 19:31:09 UTC] Checking if iox is enabled on device
[5-Nov-2021 19:31:10 UTC] Waiting for iox to be enabled on device
[5-Nov-2021 19:31:24 UTC] iox enable
[5-Nov-2021 19:31:24 UTC] iox enabled on device
[5-Nov-2021 19:31:29 UTC] Failed to install 1/1 lxc container (app-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE17.3).
Pre config validation failed. Device is not configured to accept new configuration. Available memory insufficient, required CPU:7 percent, reserved CPU:0 percent, available CPU:75 percent, required memory:2897152 KB, rese
```

In dit geval heeft de CSRv slechts 4 GB DRAM. Na de upgrade van het geheugen naar 8GB DRAM is de installatie een succes.

Controleer het huidige totale geheugen met de uitvoer van de status van het vertragingssysteem:

```
Router01# show sdwan system status
```

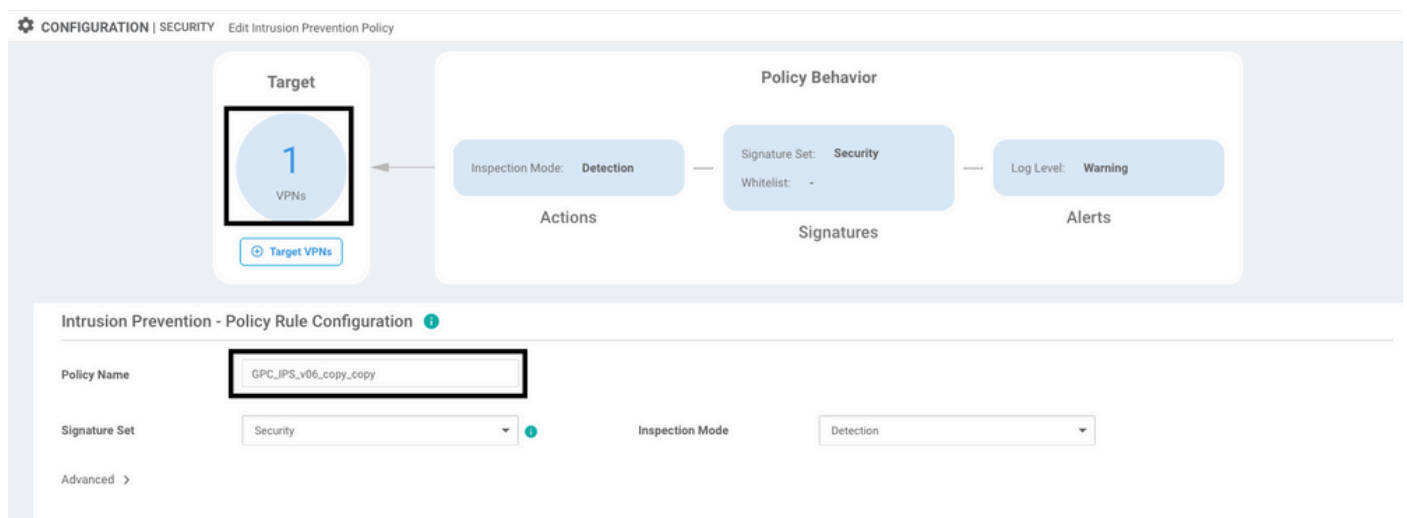
Memory usage: 8107024K total, 3598816K used, 4508208K free
349492K buffers, 2787420K cache

Probleem 3. Onrechtmatige verwijzing

Zorg ervoor dat de VPN's/VRF's die op een van de beveiligingsbeleidsfuncties worden gebruikt, al in de cEdge-router zijn geconfigureerd om een illegale verwijzing voor de beveiligingsbeleidssequenties te voorkomen.



In dit voorbeeld heeft het Beveiligingsbeleid een Inbraakpreventiebeleid voor VPN/VRF 1, maar op de apparaten is geen VRF 1 geconfigureerd. De managers sturen dus een illegale verwijzing naar die beleidsreeks.



Na het configureren van de VRF vermeld op het Beveiligingsbeleid, verschijnt de Illegale referentie niet en wordt de sjabloon met succes gedrukt.

Probleem 4. UTD is geïnstalleerd en actief maar niet ingeschakeld

Het apparaat heeft een beveiligingsbeleid geconfigureerd en UTD is geïnstalleerd en actief, maar is niet ingeschakeld.

Dit probleem houdt verband met probleem nummer 3, maar vManager stond toe dat de configuratie verwijst naar VRF's die niet in het apparaat zijn geconfigureerd en het beleid wordt niet toegepast op een VRF.

Om te bepalen of router met dit probleem te maken heeft, moet u UTD actief zien. UTD niet toegelaten bericht en het beleid maakt geen verwijzing naar enige VRF.

```
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
--------------------------	------	------	---------------------------

Controleer voor de resolutie de doel-VPN's en pas het beleid toe op een geconfigureerde VRF.

Gerelateerde informatie

- [Routerbeveiliging: Sneltoets IPS op routers](#)
- [Cisco SD-WAN security configuratiegids, Cisco IOS XE release](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.