

Installation des virtuellen UTD Security Images auf cEdge-Routern

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

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

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

[Konfigurieren](#)

[Schritt 1: Virtuelles Image hochladen](#)

[Schritt 2: Untervorlage "Sicherheitsrichtlinie und Containerprofil" zur Gerätevorlage hinzufügen](#)

[Schritt 3: Aktualisieren oder Anhängen der Gerätevorlage mit dem Sicherheitsrichtlinien- und Containerprofil](#)

[Überprüfung](#)

[Häufige Probleme](#)

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

[AUFGABE 2. Verfügbarer Speicher nicht ausreichend](#)

[AUSGABE 3. Rechtswidrige Bezugnahme](#)

[AUSGABE 4. UTD ist installiert und aktiv, aber nicht aktiviert.](#)

[Zugehörige Informationen](#)

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](#).

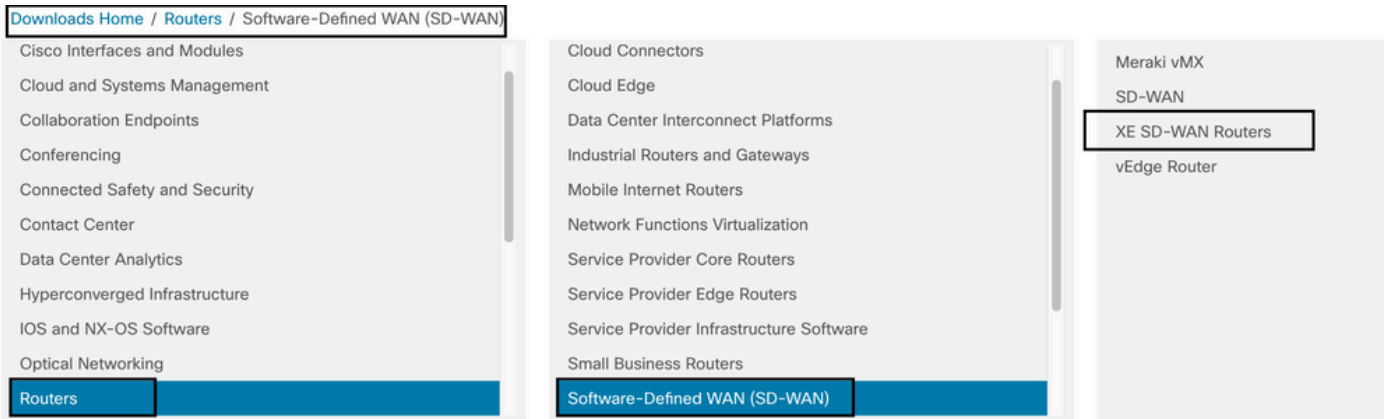
Verwenden Sie für die aktuelle Cisco IOS XE-Version den von Cisco UTD unterstützten regulären Ausdruck. Verwenden Sie den Befehl **show utd engine standard version**, um das empfohlene und unterstützte UTD-Image zu validieren.

```
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.

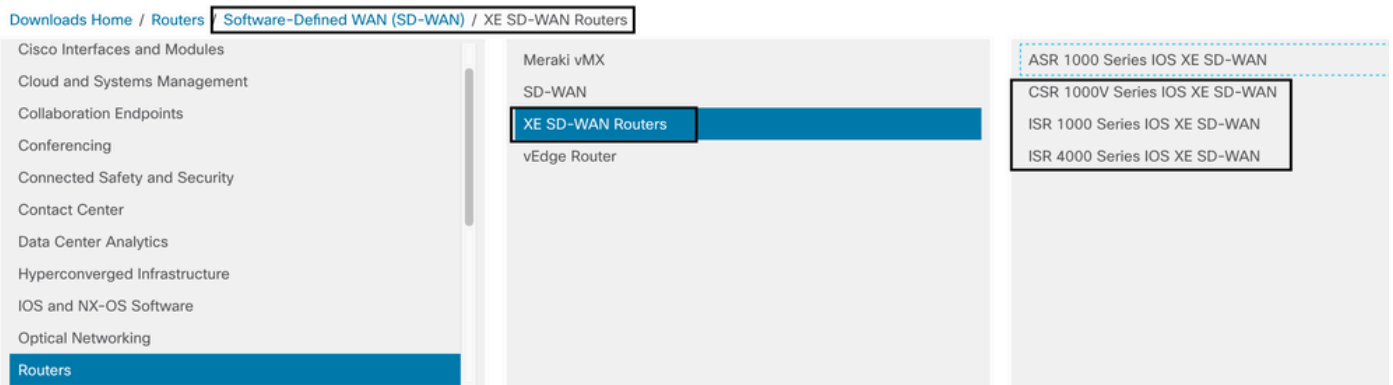
Router mit Cisco IOS XE SDWAN-Software (16.x)

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.

Q 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	↓ 🛒 📄

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.

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

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

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](#)

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

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 -

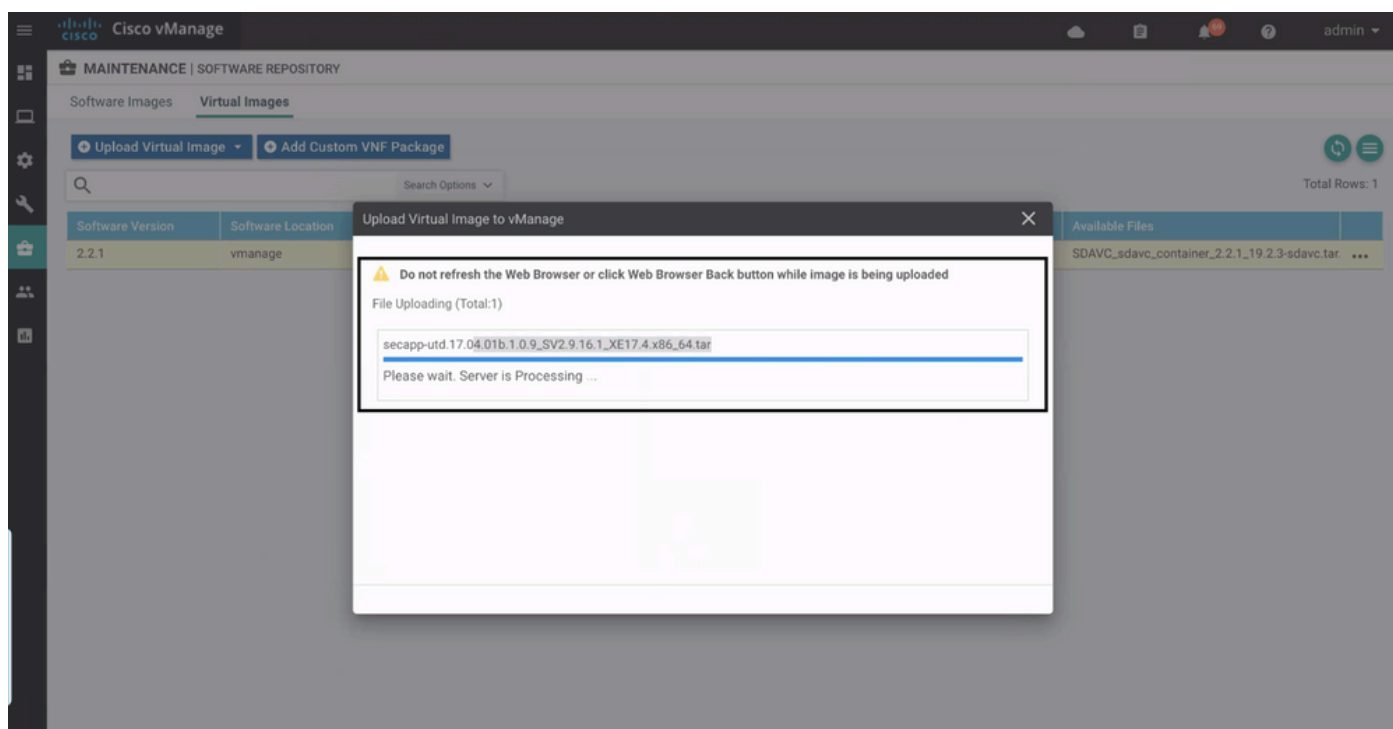
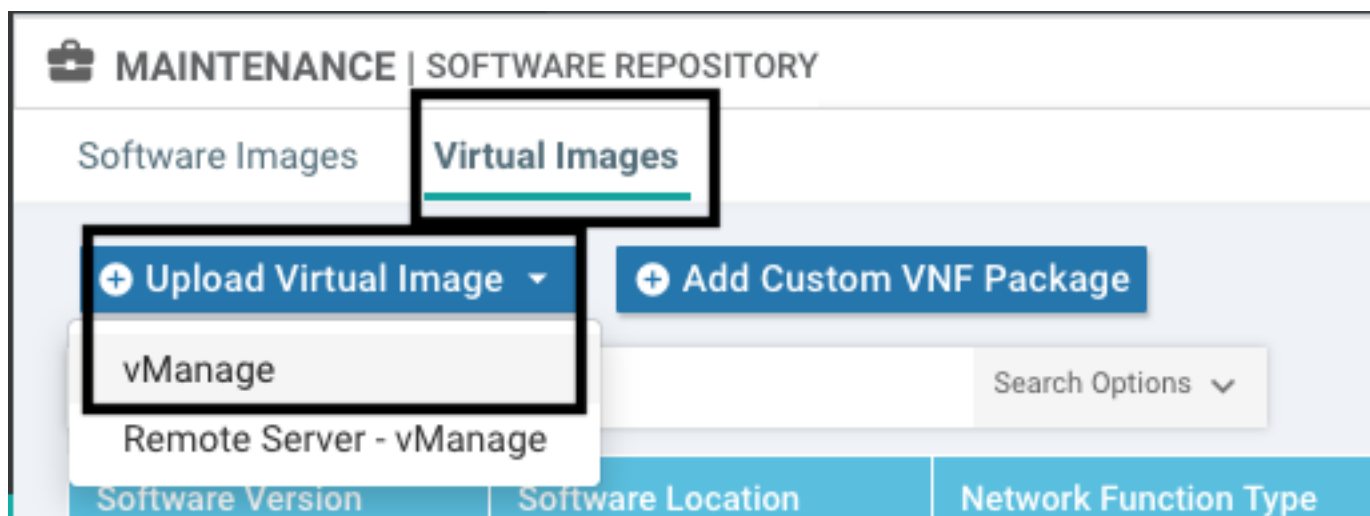
File Information	Release Date	Size
UTD Engine OVA for 17.7.1 release iosxe-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.ova Advisories	30-Nov-2021	147.72 MB
UTD Engine for IOS XE secapp-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.tar Advisories	30-Nov-2021	52.51 MB

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.



Cisco vManage MAINTENANCE | SOFTWARE REPOSITORY

Software Images Virtual Images

Upload Virtual Image Add Custom VNF Package

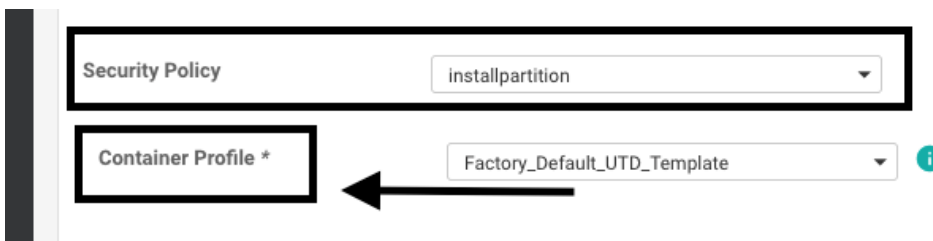
Search Options

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 ...

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.

```

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 !

```

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.

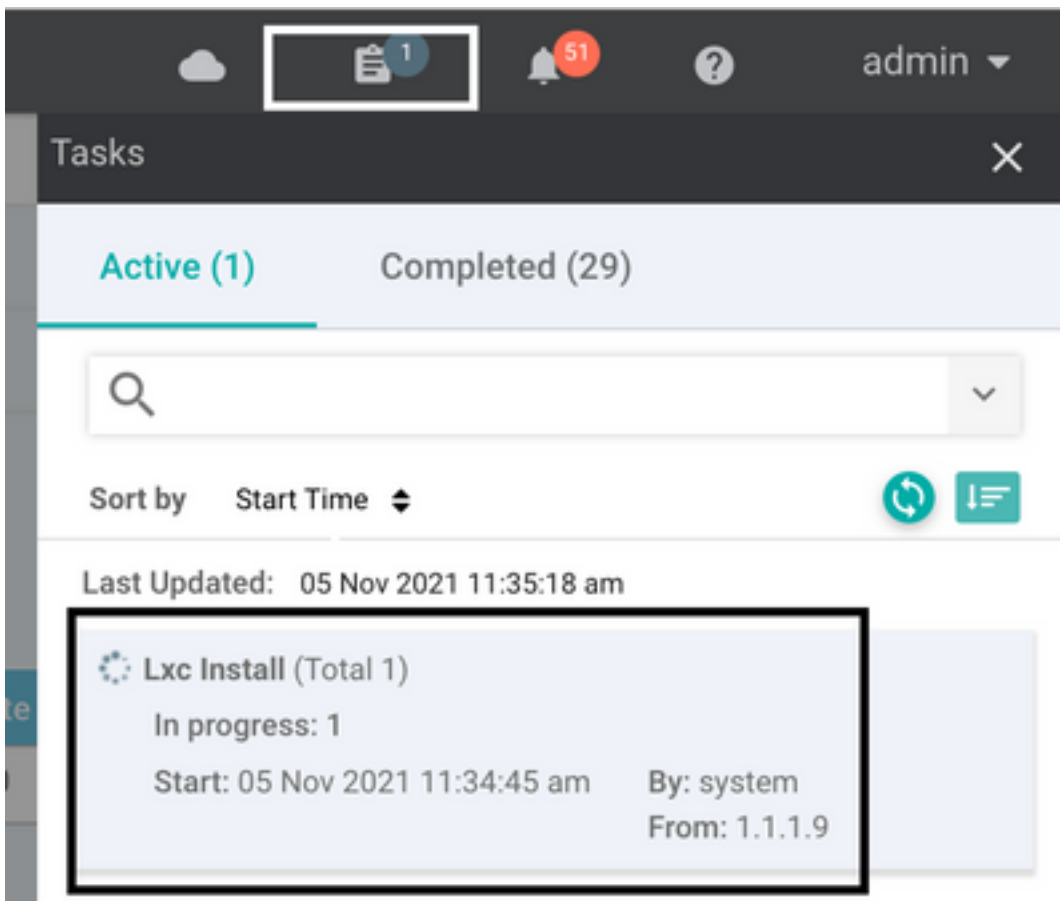
Push Feature Template Configuration | Validation Success

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

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.



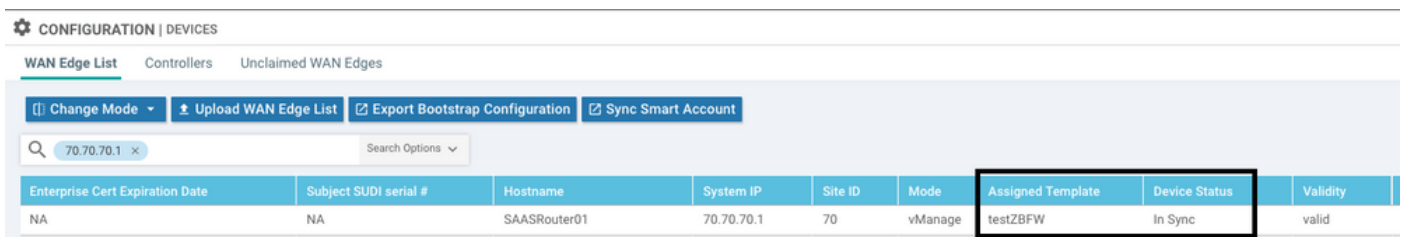
Sobald der LX-Container installiert ist, überträgt vManage die geplante Konfiguration mit den UTD-Funktionen. Hierfür ist keine neue Aufgabe vorhanden, da die Konfiguration bereits geplant war.



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**.

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

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.

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 ⓘ

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.

Add Security Policy
✕

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

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.

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:2097152 KB, rese

```

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

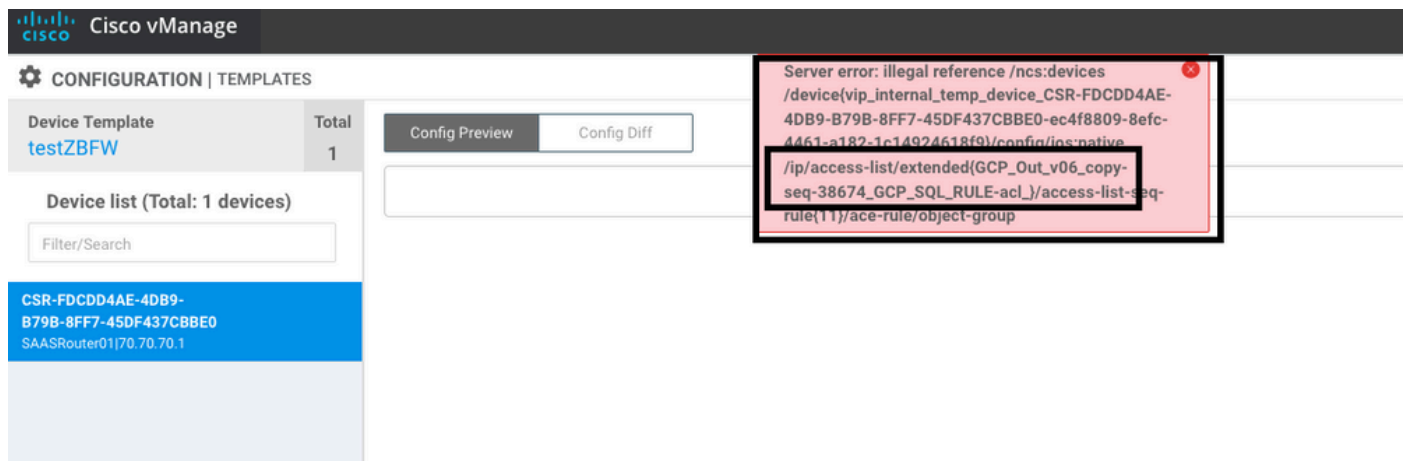
Überprüfen Sie den aktuellen Gesamtspeicher mit **show sdwan system status** output:

Router01# show sdwan system status

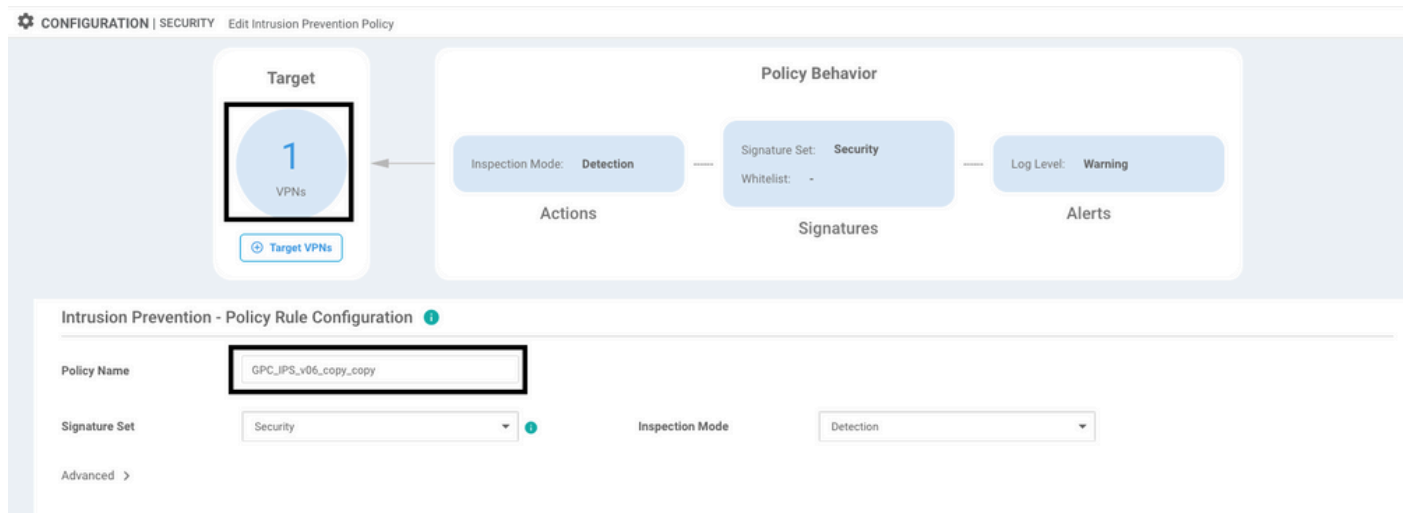
Memory usage: 8107024K total, 3598816K used, 4508208K free
349492K buffers, 2787420K cache

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.