

Install UTD Security Virtual Image on cEdge Routers

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Routers that run Cisco IOS XE SD-WAN Software \(16.x\)](#)

[Routers that run Cisco IOS XE Software \(17.x\)](#)

[Configure](#)

[Step 1. Upload Virtual Image](#)

[Step 2. Add Security Policy and Container Profile Sub-Template to Device Template](#)

[Step 3. Update or Attach the Device Template With the Security Policy and Container Profile](#)

[Verify](#)

[Common issues](#)

[ISSUE 1. Error: Following Devices do not have Container Software Services](#)

[ISSUE 2. Available Memory Insufficient](#)

[ISSUE 3. Illegal Reference](#)

[ISSUE 4. UTD is Installed and Cctive but not Enabled](#)

[Video](#)

[Related Information](#)

Introduction

This document describes how to install Unified Threat Defense (UTD) Security Virtual Image to enable security features on Cisco IOS® XE SD-WAN Devices.

Prerequisites

- Before you use these features, upload the relevant Security Virtual Image to vManage repository.
- Cisco Edge router must be on vmanage mode with template pre attached.
- Create a Security Policy Template for Intrusion Prevention System (IPS), Intrusion Detection System (IDS), URL Filtering (URL-F), or Advanced Malware Protection (AMP) Filtering.

Requirements

- 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)
- Cisco Edge platforms that support 8GB DRAM.

Components Used

- Cisco UTD Virtual Image
- vManage controller
- Cisco Edge routers with control connections with controllers.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Cisco UTD image needs a Security policy on the device template to be installed, and security features enabled such as Intrusion Prevention System (IPS), Intrusion Detection System (IDS), URL Filtering (URL-F), and Advanced Malware Protection (AMP) on Cisco Edge routers.

Download the Cisco UTD Snort IP Engine software from [Software Cisco](#)

Use the Cisco UTD virtual image supported regex for the current Cisco IOS XE version. Use the command **show utd engine standard** version to validate the recommended and supported UTD image.


```
<#root>
```

```
Router01#
```

```
show utd engine standard version
```

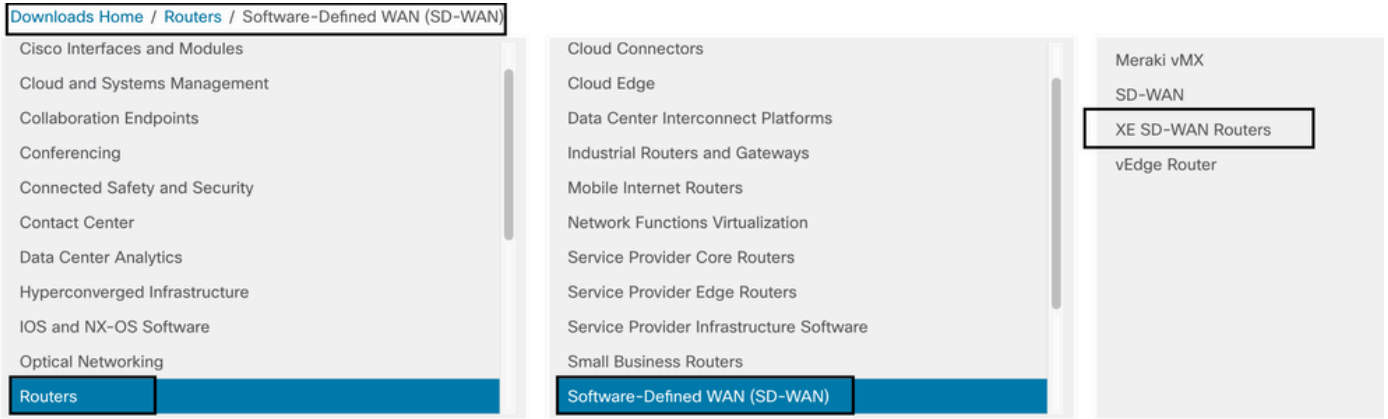
```
IOS-XE Recommended UTD Version: 1.0.13_SV2.9.16.1_XE17.3
```

```
IOS-XE Supported UTD Regex: ^1\.0\.[([0-9]+)_SV(.*)_XE17.3$
```

 **Note** The path to download the image depends if the router runs Cisco IOS XE SD-WAN Software (16.x) or Universal Cisco IOS XE software (17.x).

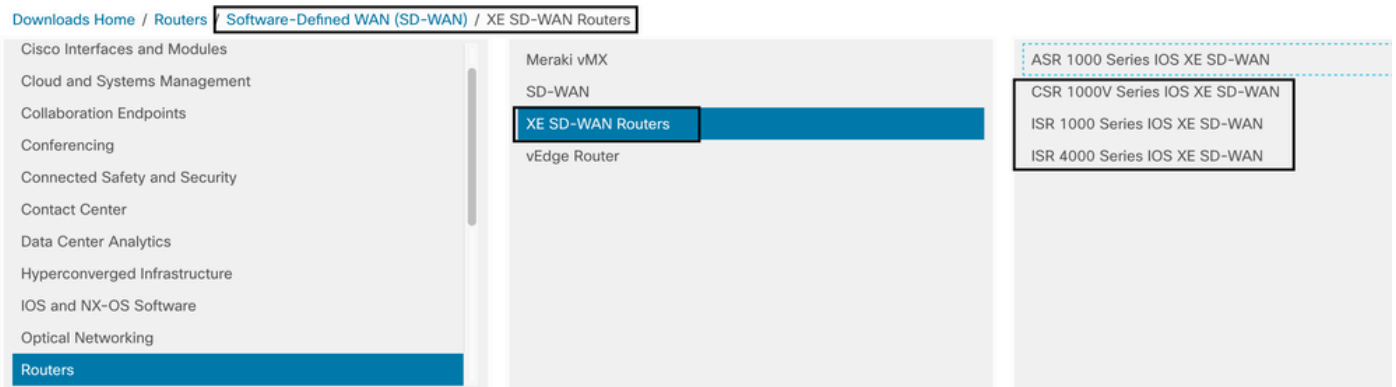
Routers that run Cisco IOS XE SD-WAN Software (16.x)

The path to get the Cisco UTD Snort IPS Engine software is Routers/ Software-Defined WAN (SD-WAN)/ XE SD-WAN Routers / and the Series Integrated Router.

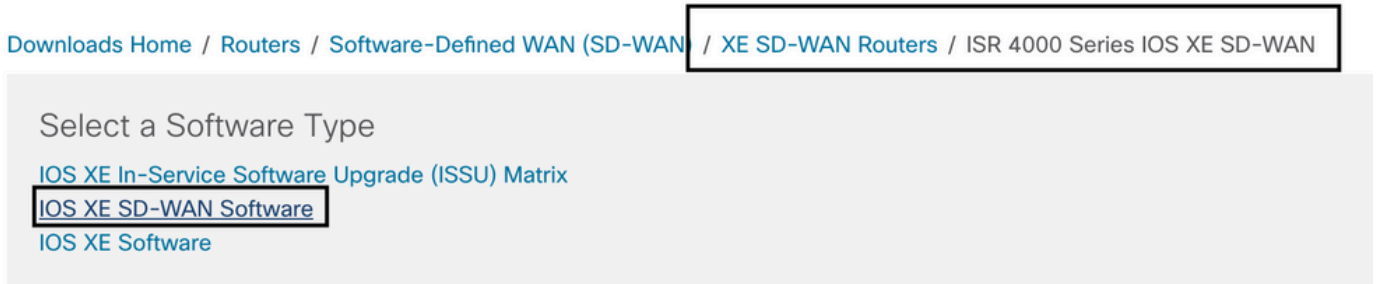



Choose the model type for the Cisco Edge router.

 **Note** Series Aggregation Services Routers (ASR) are not available for UTD Features.



After you choose the type router model, select the **Cisco IOS XE SD-WAN software** option to get the UTD package for Cisco Edges on 16.x version.



 **Note** The download path to choose the Cisco UTD virtual image for 16.x code for Cisco Edge routers shows also **Cisco IOS XE software** option. That is the path to choose upgrade codes of Cisco Edge for 17.x only, but there is not located the UTD virtual image for version 17.x. Cisco unified regular Cisco IOS XE and Cisco IOS XE SD-WAN codes on 17.x and latest, so the path to get the Cisco UTD virtual image for 17.x is the same as regular Cisco IOS XE codes.

Choose the current version of the Cisco Edge, and download the UTD package for that version.

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 that run Cisco IOS XE Software (17.x)

Cisco IOS XE Release 17.2.1r, and the latest use the universalk9 image to deploy both Cisco IOS XE SD-WAN and Cisco IOS XE on Cisco IOS XE devices.

UTD Snort IPS Engine software is located in **Routers > Branch Routers > Series Integrated 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

After you choose the model type of the router, select the **UTD Snort 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](#)

Select the current version of the router, and download the UTD package for version selected.

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 -

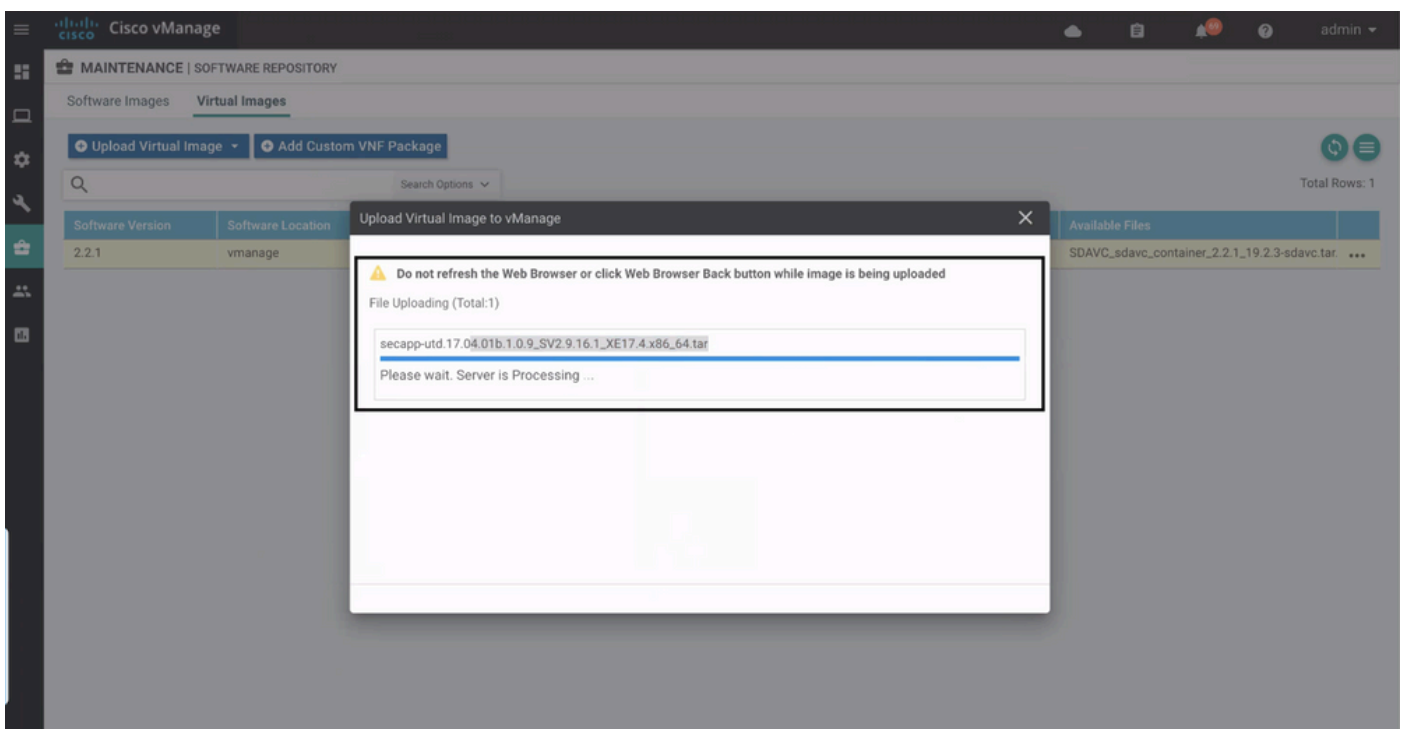
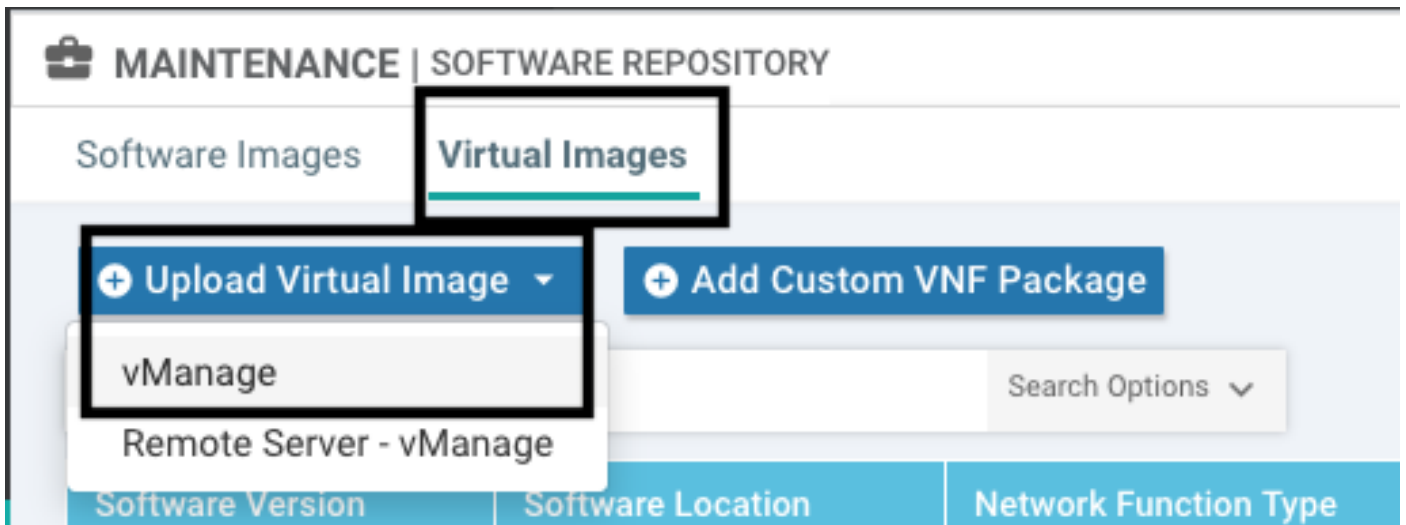
File Information	Release Date	Size
UTD Engine OVA for 17.7.1 release iosxe-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.ova Advisories	30-Nov-2021	147.72 MB
UTD Engine for IOS XE secapp-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.tar Advisories	30-Nov-2021	52.51 MB

 **Note:** Cisco ISR1100X Series Routers (Cisco Nutella Routers SR1100X-4G/6G) that run Cisco IOS XE Software instead of Viptela Code are based on x86_x64. The Cisco UTD virtual image published for ISR4K can work on them. You can install the same Cisco UTD image code version supported regex for the current Cisco IOS XE SD-WAN version on the Nutella router. Use the command **show utd engine standard version** to validate the recommended and supported regex Cisco UTD image.

Configure

Step 1. Upload Virtual Image

Ensure your virtual image matches with the current Cisco IOS XE SD-WAN code on the Cisco Edge and upload it in to vmanage repository.
Navigate to **Maintenance > Software Repository > Virtual Image > Upload Virtual Image > vManage**.



Once the Cisco UTD virtual image was successfully uploaded, double check it is on the repository.



Cisco vManage MAINTENANCE | SOFTWARE REPOSITORY

Software Images Virtual Images

Upload Virtual Image Add Custom VNF Package

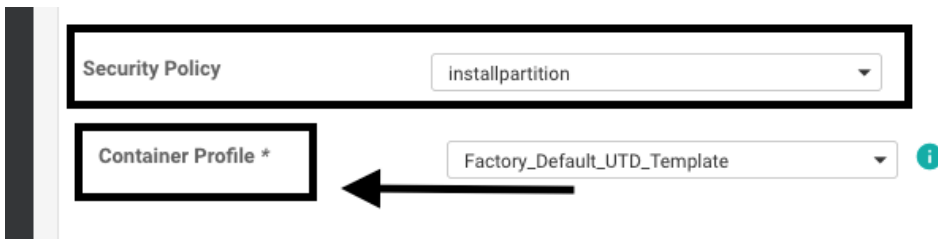
Search Options

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 ...

Step 2. Add Security Policy and Container Profile Sub-Template to Device Template

Add the security policy previously created to the device template. The security policy must have a IPS/IDS, URL-F, or AMP Filtering policy on it to the device template. Open the container profile automatically. Use the default container profile or modify it if needed.



Step 3. Update or Attach the Device Template With the Security Policy and Container Profile

Update or attach the template to the Cisco Edge router. Notice on config diff that the app-hosting configuration and UTD engine for the feature IPS/IDS, URL-F, or AMP Filtering is configured.

```

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 !ldp run
259 nat64 translation timeout tcp 60
260 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 !

```

Template status change to **Done-scheduled** due the vmanage noticed that the configuration applied has UTD engine features, so vmanage determine that the Cisco Edge needs the Virtual Image installed to use the UTD security features.

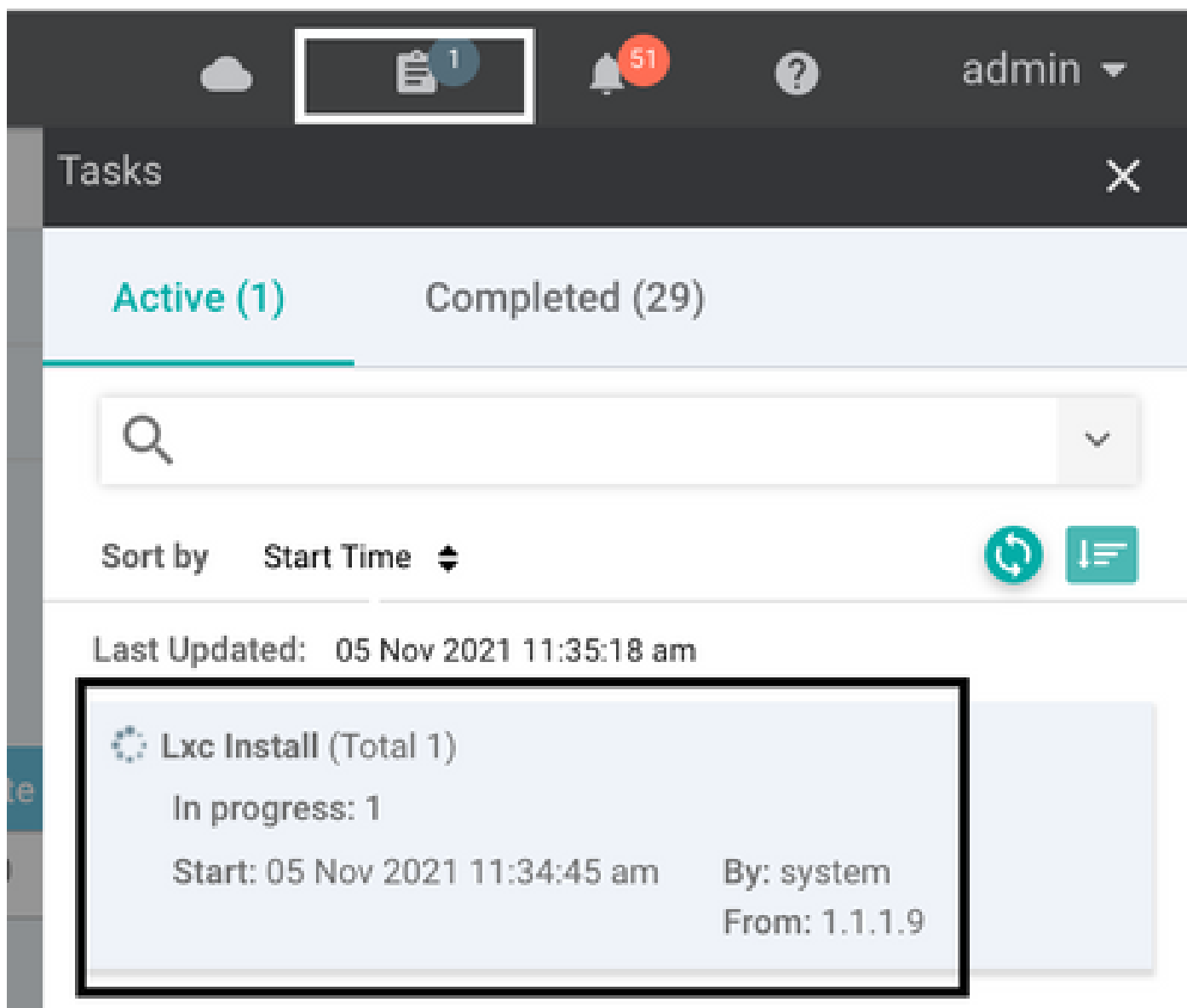


Push Feature Template Configuration | Validation Success

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


After the template is moved to the schedule state, a new task **in progress** appears in the task menu. The new task is the **Lxc installation**, it means that the vmanage starts automatically the installation of the virtual image to the Cisco Edge before push the new configuration.



Tasks

Active (1) Completed (29)

Last Updated: 05 Nov 2021 11:35:18 am

 Lxc Install (Total 1)	
In progress: 1	
Start: 05 Nov 2021 11:34:45 am	By: system
	From: 1.1.1.9

Once the LX container is installed, the vManage push the pre-schedule configuration with the UTD features. There is not a new task for this due the configuration was previously scheduled.

URL Filtering : Enabled

<<<<<<<<<<<<<<

File Inspection : Enabled

<<<<<<<<<<<<<<

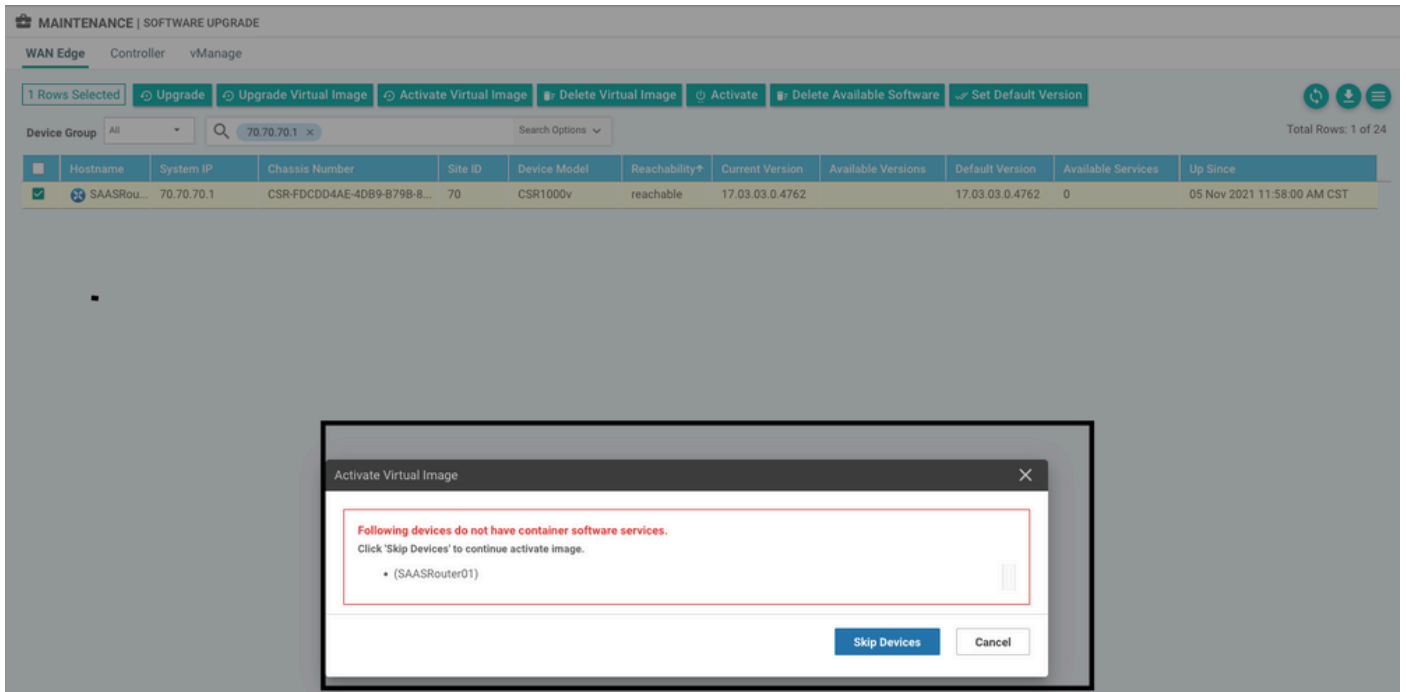
All Interfaces : Enabled

Common issues

ISSUE 1. Error: Following Devices do not have Container Software Services

Activate the virtual image.

Navigate to **maintenance > software > activate**



The virtual image send an error: **Devices so not have container software revices**, If the Cisco Edge router selected does not have a security policy with the container profile sub-template.

Additional Templates

AppQoE

Global Template * ⓘ

Cisco Banner

Cisco SNMP

CLI Add-On Template

Policy

Probes

Security Policy



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 * ⓘ





This template is automatically added if you use a Security Policy that includes security features such as Intrusion Prevention System (IPS), Intrusion Detection System (IDS), URL Filtering (URL-F), and Advanced Malware Protection (AMP) that needs UTD package. Not all the Security features available needs UTD engine such like simple ZBFW feature.


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

Once you push the template with the container profile sub-template, the vmanage automatically install the virtual image.

ISSUE 2. Available Memory Insufficient

Make sure the Cisco Edge router has 8 GB DRAM memory, if not, the Lxc Install process send a **Device is not configured to accept new configuration. Available memory insufficient** error. The requirements for Cisco Edge routers to use UTD features is to have minimum of 8 GB of DRAM.

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
  
```

On this case, the CSRv have only 4 GB of DRAM. After upgrade of the memory to 8GB DRAM, the installation is a success.


Verify the current total memory with **show sdwan system status** output:

```
<#root>
```

```
Router01#
```

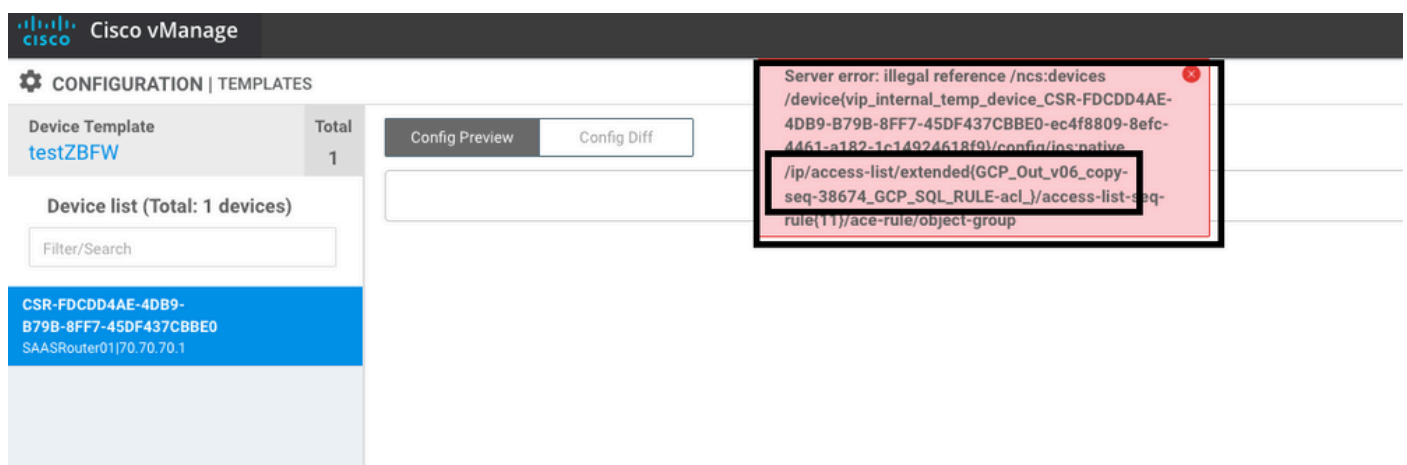
```
show sdwan system status
```

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

 **Note** Sufficient free memory must be available to install UTD. If the installed DRAM is adequate but installation is still failing due to lack of memory, check current usage in **show processes memory platform sorted**

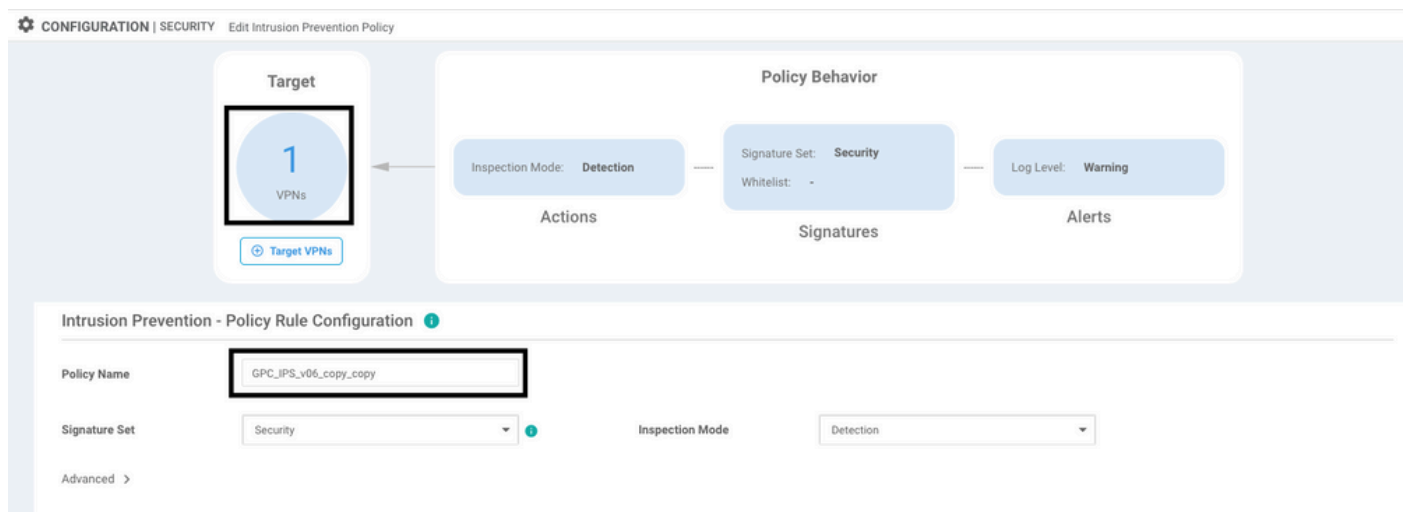
ISSUE 3. Illegal Reference

Make sure that the VPNs/VRFs used on any of the Security Policy features are already configured in the Cisco Edge router to avoid an illegal reference for the Security Policy sequences.



The screenshot shows the Cisco vManage interface. On the left, under 'CONFIGURATION | TEMPLATES', there is a 'Device Template' section for 'testZBFW' with a total of 1 device. Below it is a 'Device list (Total: 1 devices)' with a search filter and a table listing the device: 'CSR-FDCDD4AE-4DB9-B79B-8FF7-45DF437CBBE0 SAASRouter01[70.70.70.1]'. On the right, there are 'Config Preview' and 'Config Diff' buttons. A red error message box is overlaid on the right side, containing the text: 'Server error: illegal reference /ncs:devices /device(vip_internal_temp_device_CSR-FDCDD4AE-4DB9-B79B-8FF7-45DF437CBBE0-ec4f8809-8efc-4461-a182-1c14924618f9)/config/ips-native /ip/access-list/extended(GCP_Out_v06_copy-seq-38674_GCP_SQL_RULE-acl_)/access-list-seq-rule(11)/ace-rule/object-group'. The error message is highlighted with a red border.

In this example, the Security Policy has an Intrusion Prevention Policy for VPN/VRF 1, but the devices does not have any VRF 1 configured. So, the vmanage send an illegal reference for that policy sequence.



The screenshot shows the Cisco vManage interface for 'Edit Intrusion Prevention Policy'. The 'Target' section shows '1 VPNs' with a 'Target VPNs' button. The 'Policy Behavior' section shows 'Inspection Mode: Detection', 'Signature Set: Security', and 'Log Level: Warning'. Below this is the 'Intrusion Prevention - Policy Rule Configuration' section, which includes a 'Policy Name' field with the value 'GPC_IPS_v06_copy_copy', a 'Signature Set' dropdown menu set to 'Security', and an 'Inspection Mode' dropdown menu set to 'Detection'. The 'Policy Name' field is highlighted with a black border.

After configure the VRF mentioned on the Security Policies, the Illegal reference does not appear and the template is pushed successfully.

ISSUE 4. UTD is Installed and Cctive but not Enabled

The device has a security policy configured, and UTD is installed and active but it is not enabled.

This issue is related to issue number 3, nevertheless, vManage allowed the configuration to make reference to VRFs that are not configured in the device and the policy is not applied to any VRF.

To determine if router faces this issue, you need to see UTD active. UTD not enabled message and the policy does not make reference to any VRF.

```
<#root>
```

```
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

For the resolution, verify the target VPNs and make sure to apply the policy to a VRF configured.

Video

[Install UTD Security Virtual Image on cEdge Routers](#)

Related Information

- [Router Security: Snort IPS on Routers](#)
- [Cisco SD-WAN Security Configuration Guide, Cisco IOS XE Release](#)
- [Technical Support & Documentation - Cisco Systems](#)