Install UTD Security Virtual Image on cEdge Routers

Contents

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#
```

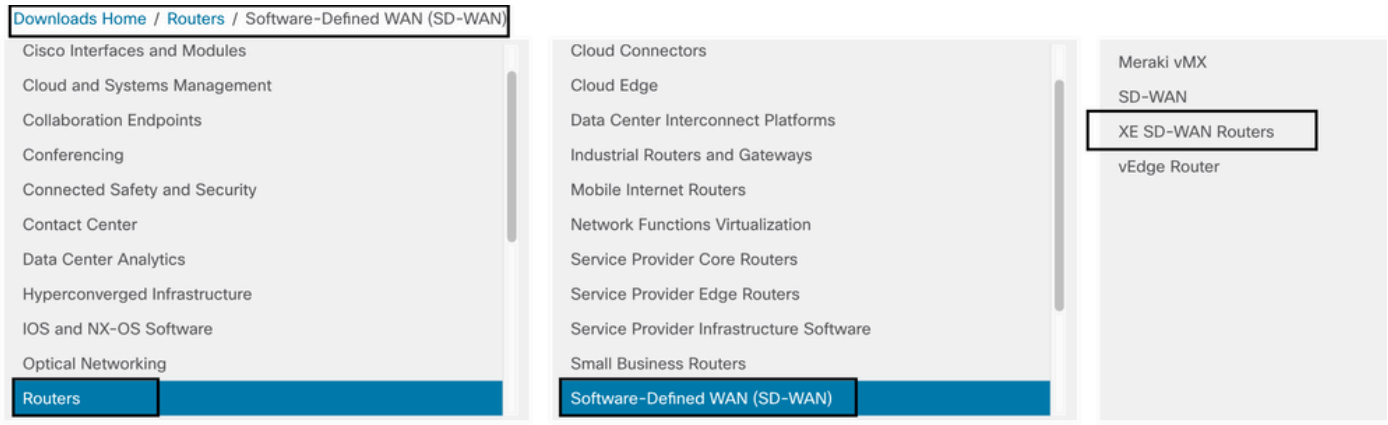
```
show utd engine standard version
```

```
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).

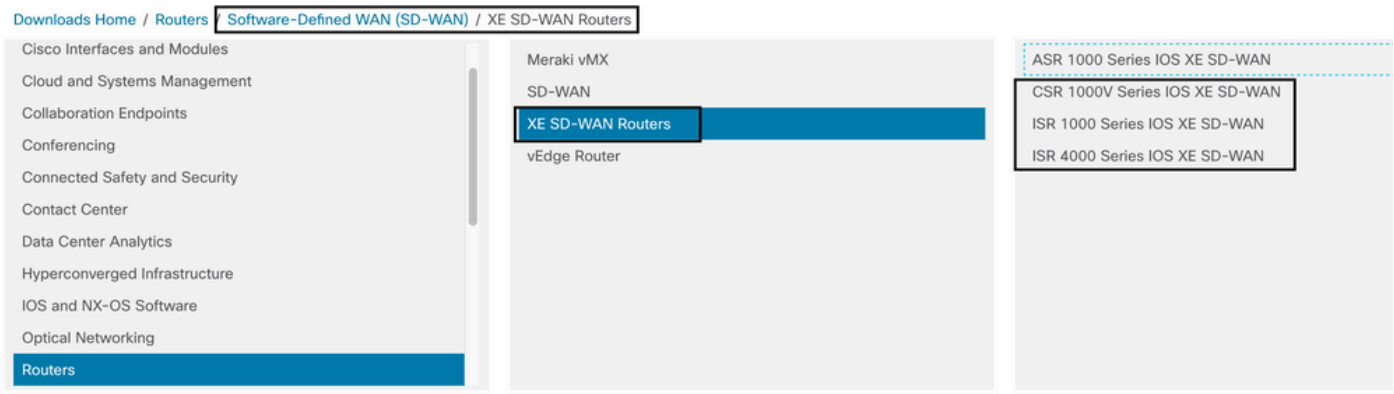
Routers that run Cisco IOS XE SD-WAN Software (16.x)

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.

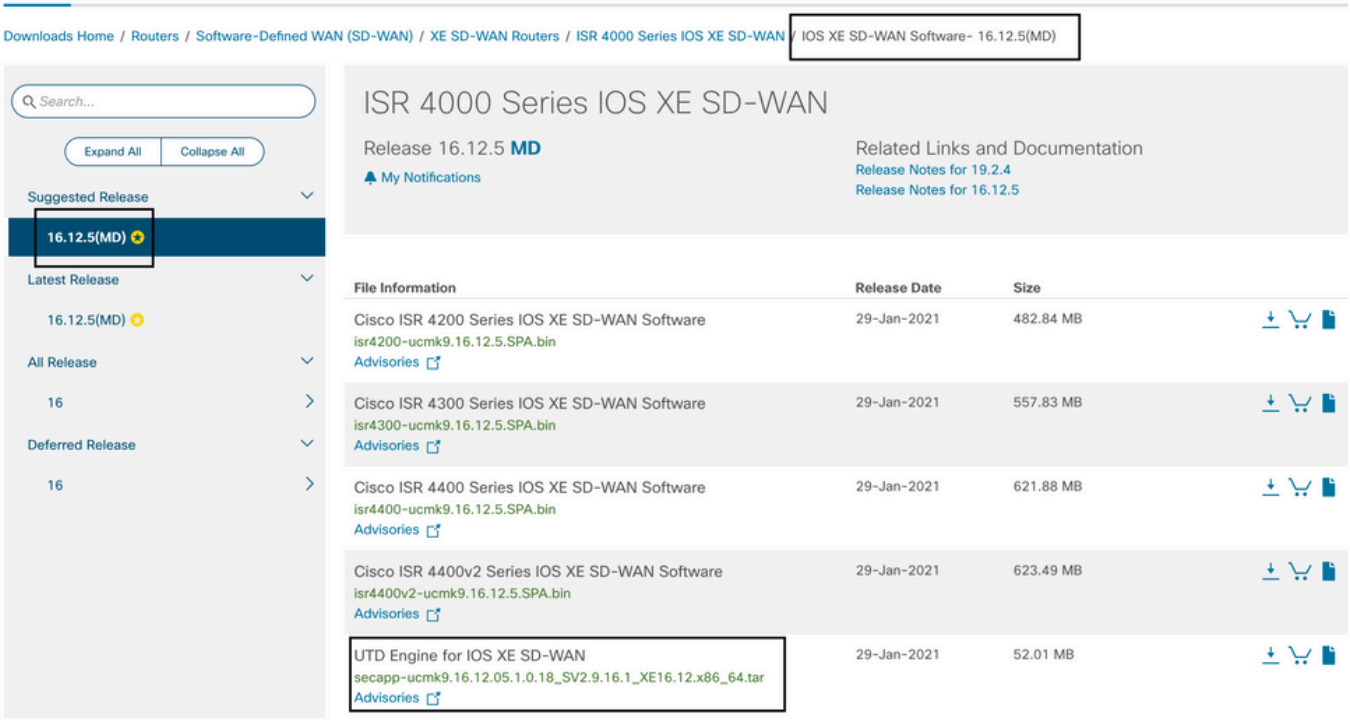
Note Series Aggregation Services Routers (ASR) are not available for UTD Features.



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.

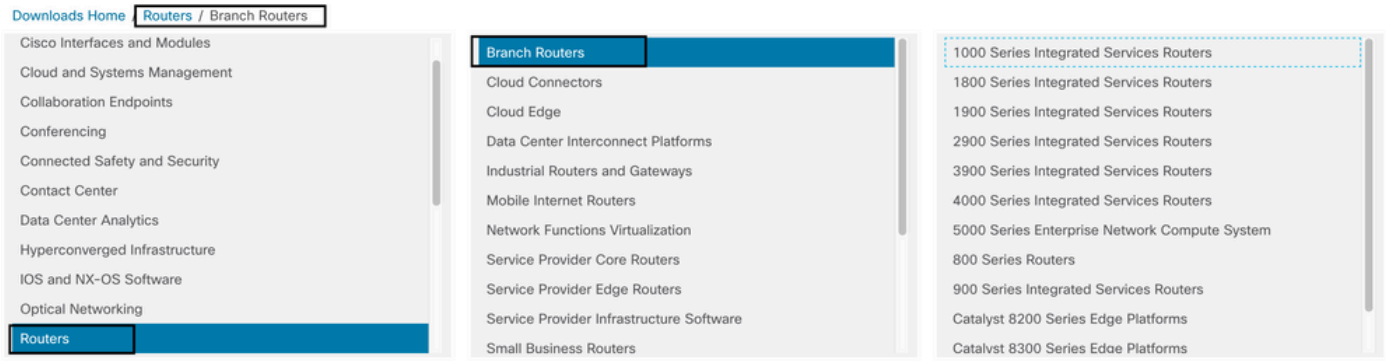
Note The download path to chose the Cisco UTD virtual image for 16.x code for Cisco Edge routers shows also **Cisco IOS XE software** option. That is the path to choose upgrade codes of Cisco Edge for 17.x only, but there is not located the UTD virtual image for version 17.x. Cisco unified regular Cisco 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.

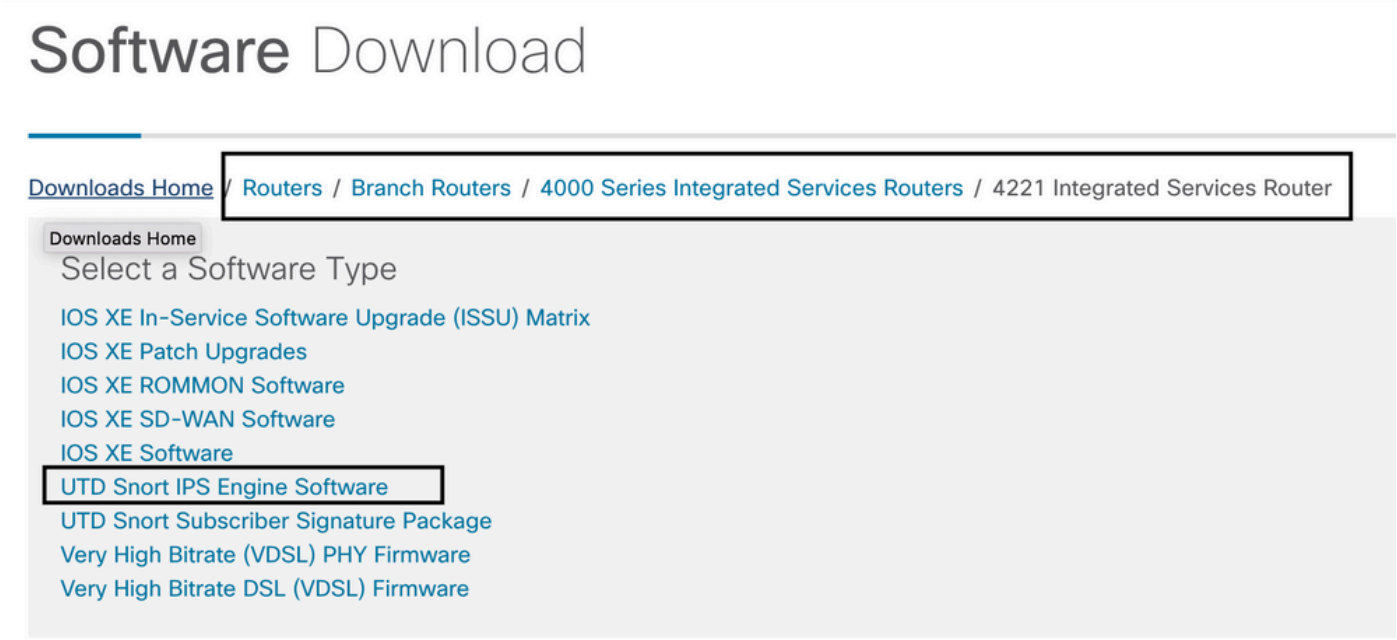


Routers that run Cisco IOS XE Software (17.x)

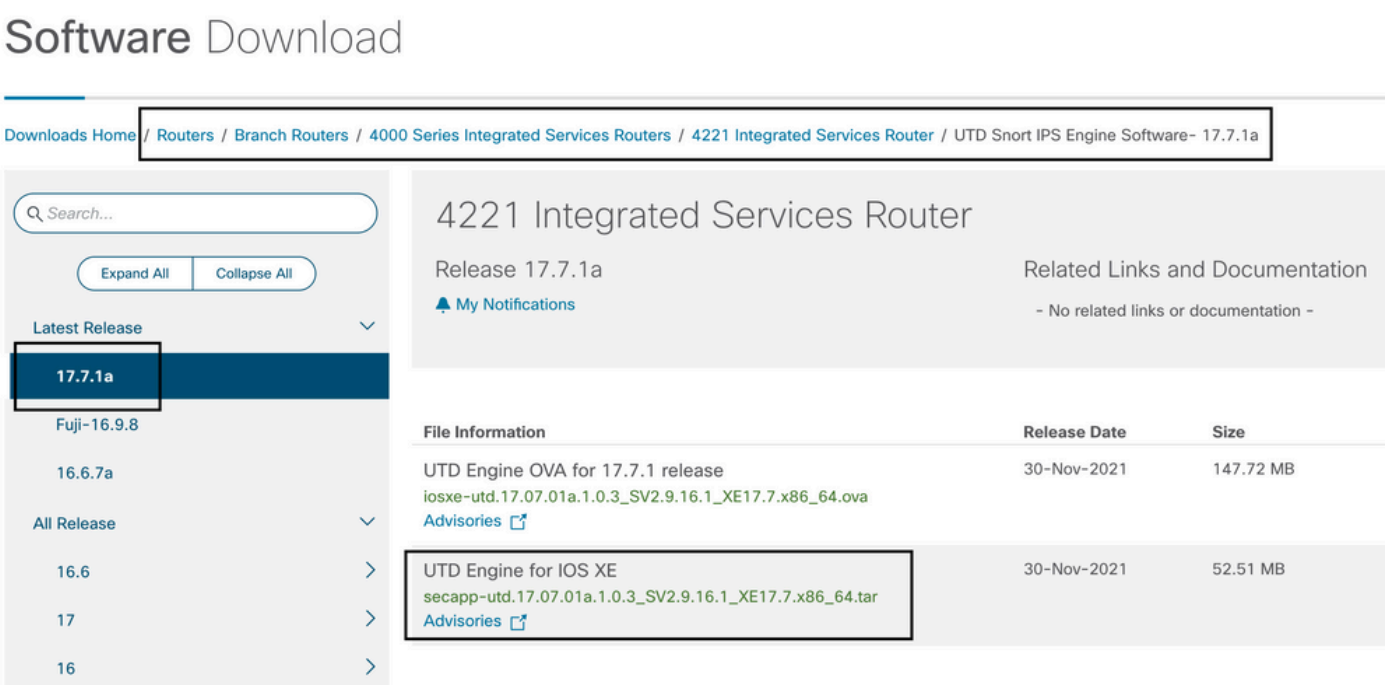
Cisco IOS XE Release 17.2.1r, and the latest use the universalk9 image to deploy both Cisco IOS XE SD-WAN and Cisco IOS XE on Cisco IOS XE devices.
UTD Snort IPS Engine software is located in **Routers > Branch Routers > Series Integrated Router**.



After you choose the model type of the router, select the **UTD Snort IPS Engine Software**.



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

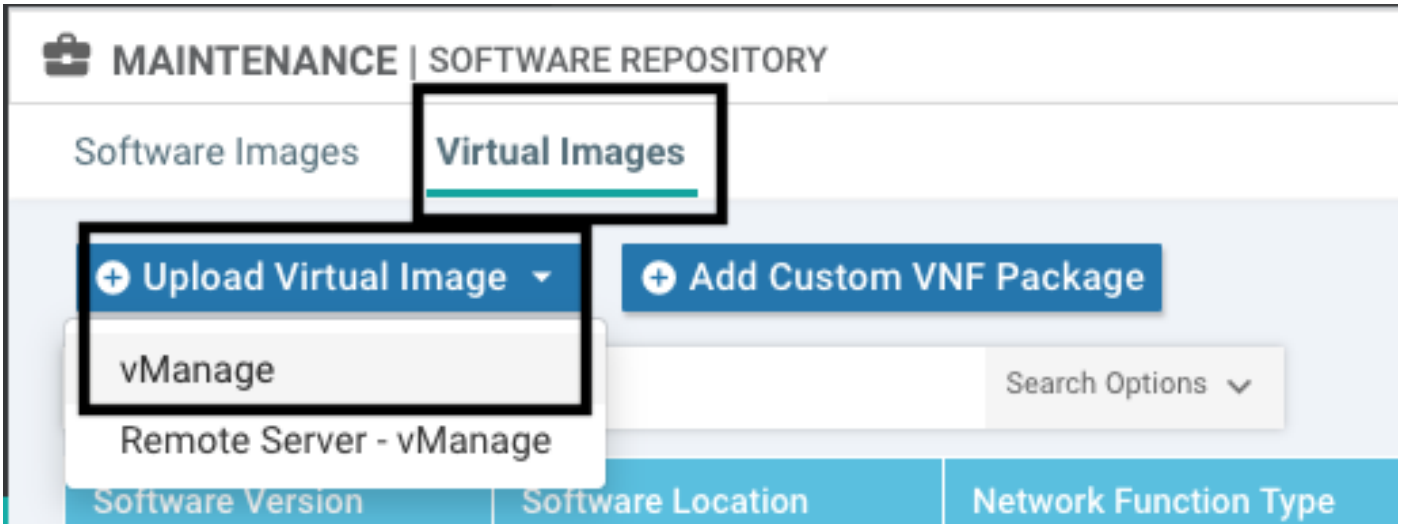


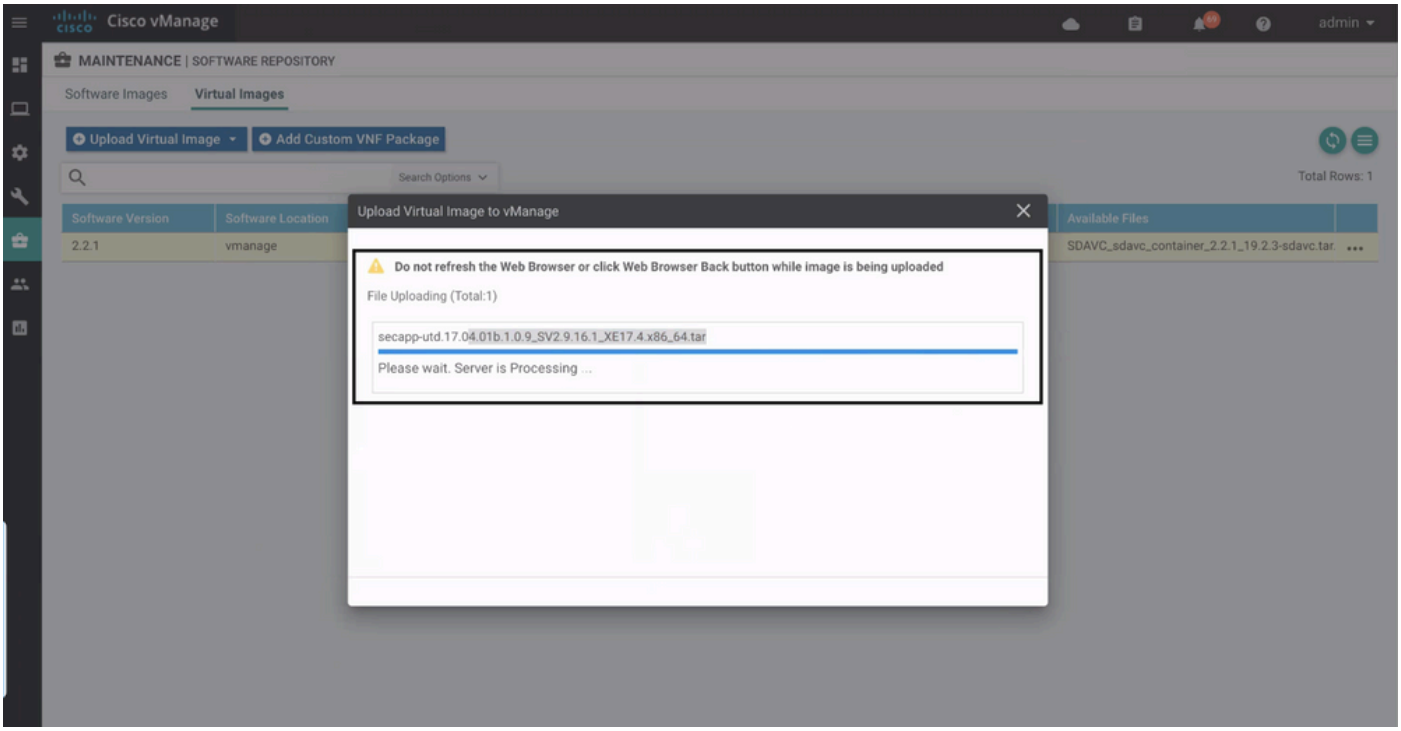
Note: Cisco ISR1100X Series Routers (Cisco Nutella Routers SR1100X-4G/6G) that run Cisco IOS XE Software instead of Viptela Code are based on x86_x64. The Cisco UTD virtual image published for ISR4K can work on them. You can install the same Cisco UTD image code version supported regex for the current 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

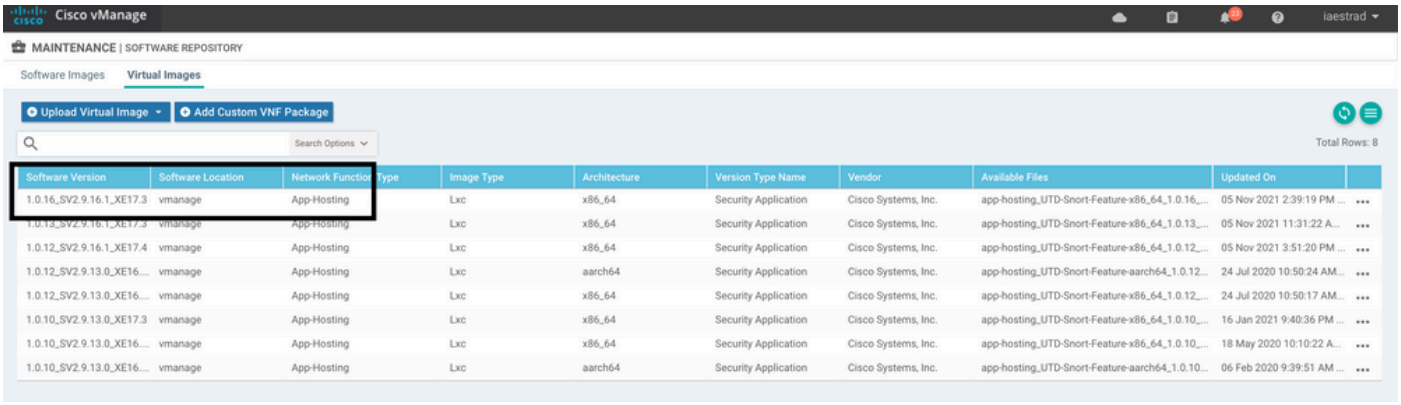
Step 1. Upload Virtual Image

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.**



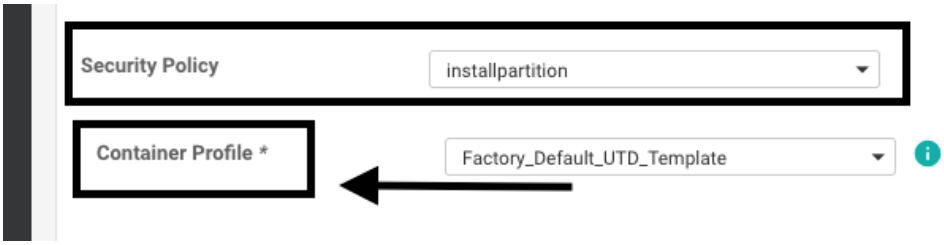


Once the Cisco UTD virtual image was successfully uploaded, double check it is on the repository.



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

Add the security policy previously created to the device templete. 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.

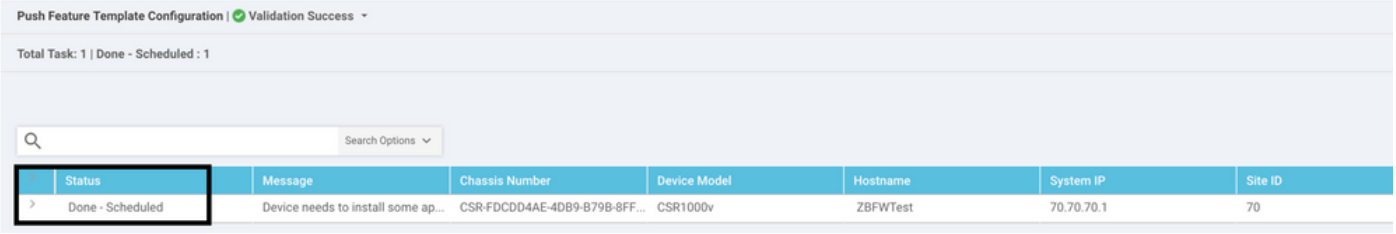


Step 3. Update or Attach the Device Template With the Security Policy and Container Profile

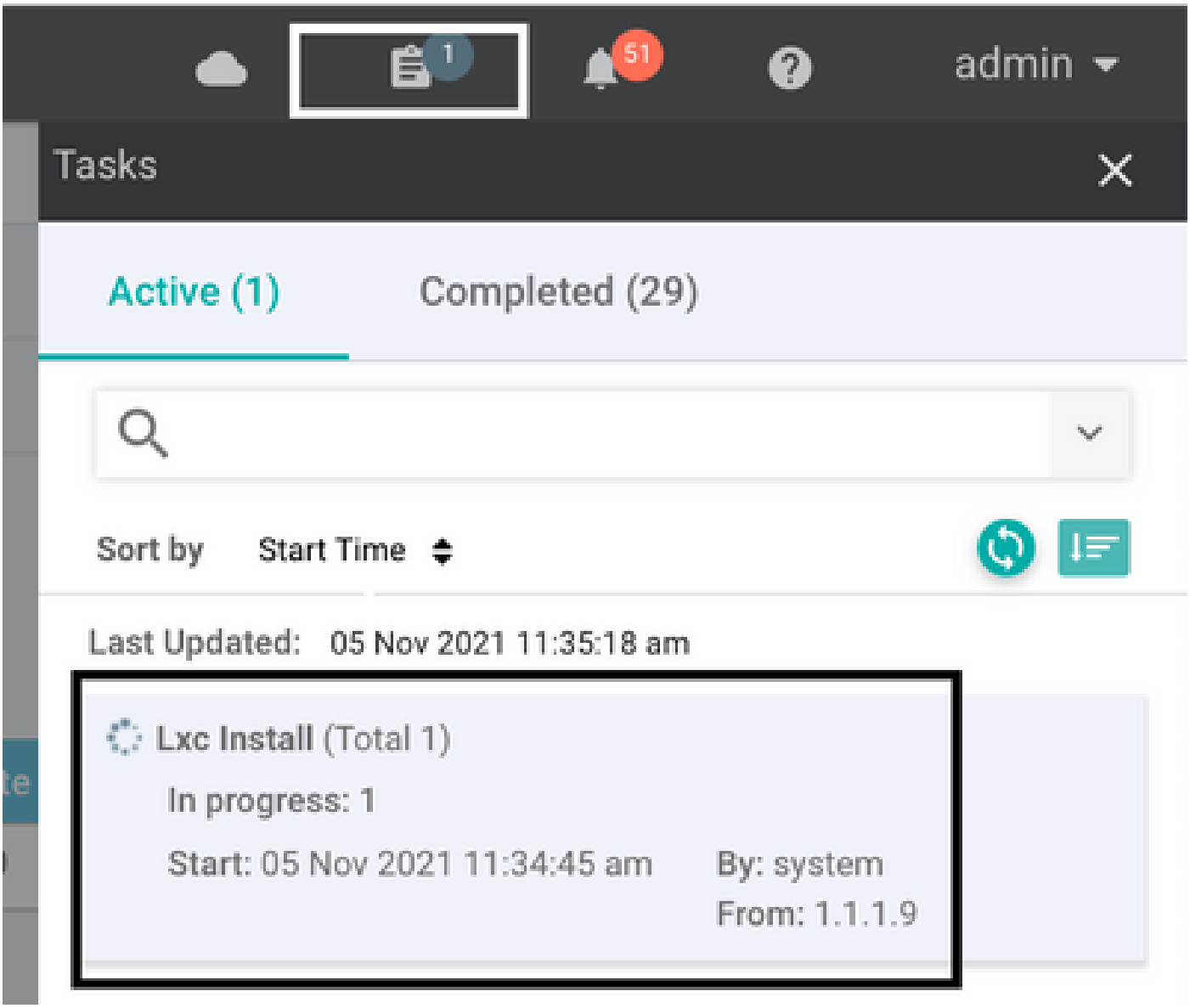
Update or attach the template to the Cisco Edge router. Notice on config diff that the app-hosting configuration and UTD engine for the feature IPS/IDS, URL-F, or AMP Filtering is configured.

```
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 !
258 268 lldp 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 !
```

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.



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.

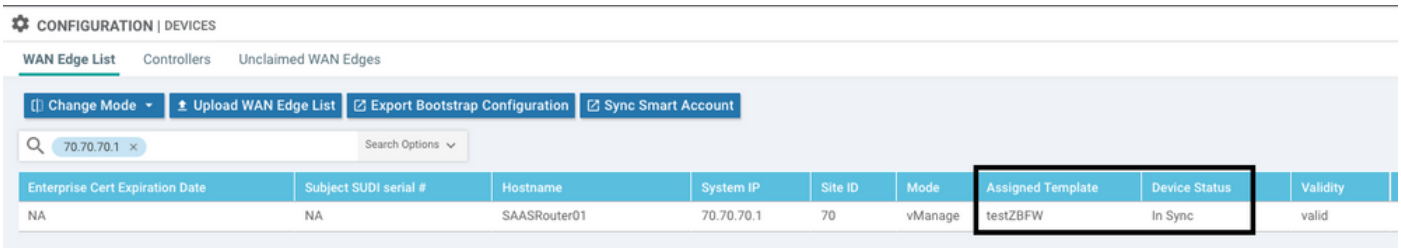


Once the LX container is installed, the vManage push the pre-schedule configuration with the UTD features. There is not a new task for this due the configuration was previously scheduled.

Verify

Verify if the Cisco Edge is in sync with vManage and template attached.

Navigate to **Configuration > Devices**



Verify if the Cisco UTD version is installed:

<#root>

```
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
```

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

Note UTD Installed version cannot be on **UNSUPPORTED** state.

Check if UTD is on **running** state with next output:

<#root>

```
Router02#
```

show app-hosting list

```
App id                                   State
```

```
------------------------------------------------------------
utd                                      RUNNING

<<<<<<<<<<<<<<<<<<
```

The next command summarizes the previous commands and shows the current status and version:

```
<#root>

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
```

Show utd engine standard status command shows the health status of the UTD engine and list time it get the signature update.

```
<#root>

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
```

Verify the features enabled use the next command:

```
<#root>

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
```

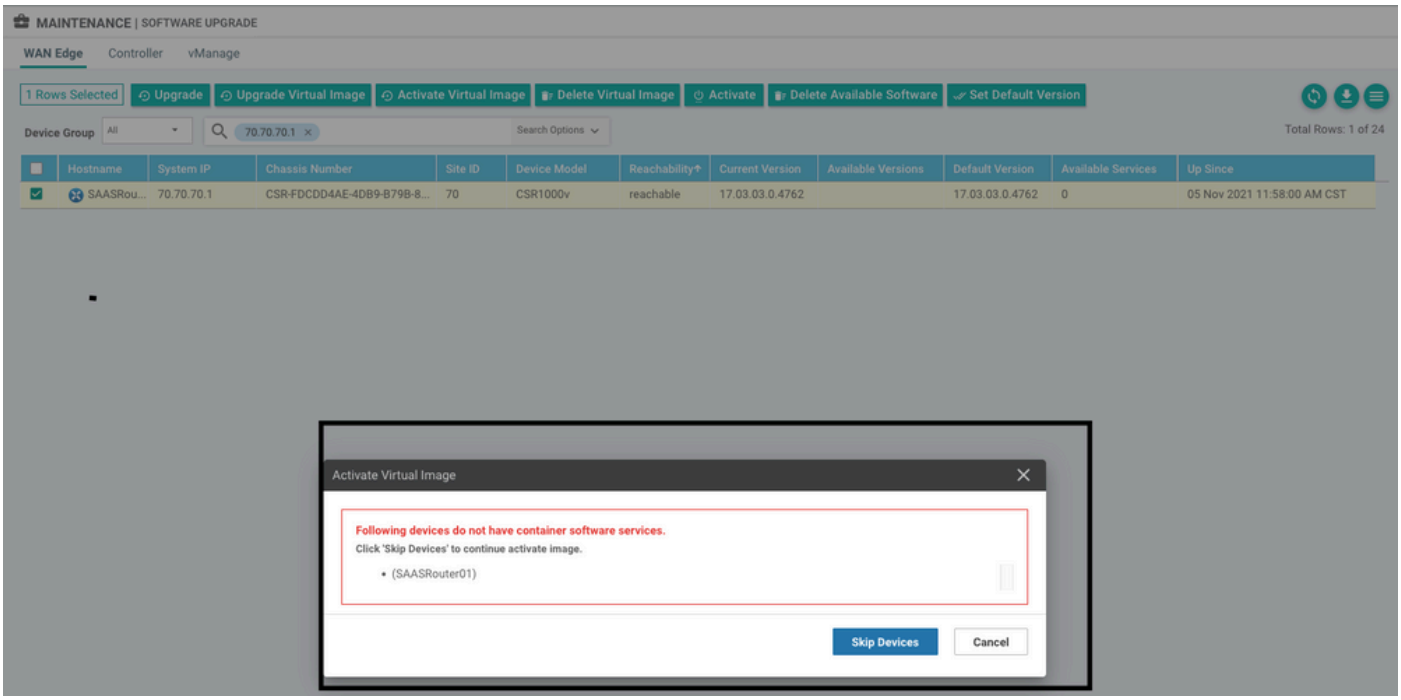
```
        URL Filtering     : Enabled
<<<<<<<<<<<
        File Inspection   : Enabled
<<<<<<<<<<<
        All Interfaces    : Enabled
```

Common issues

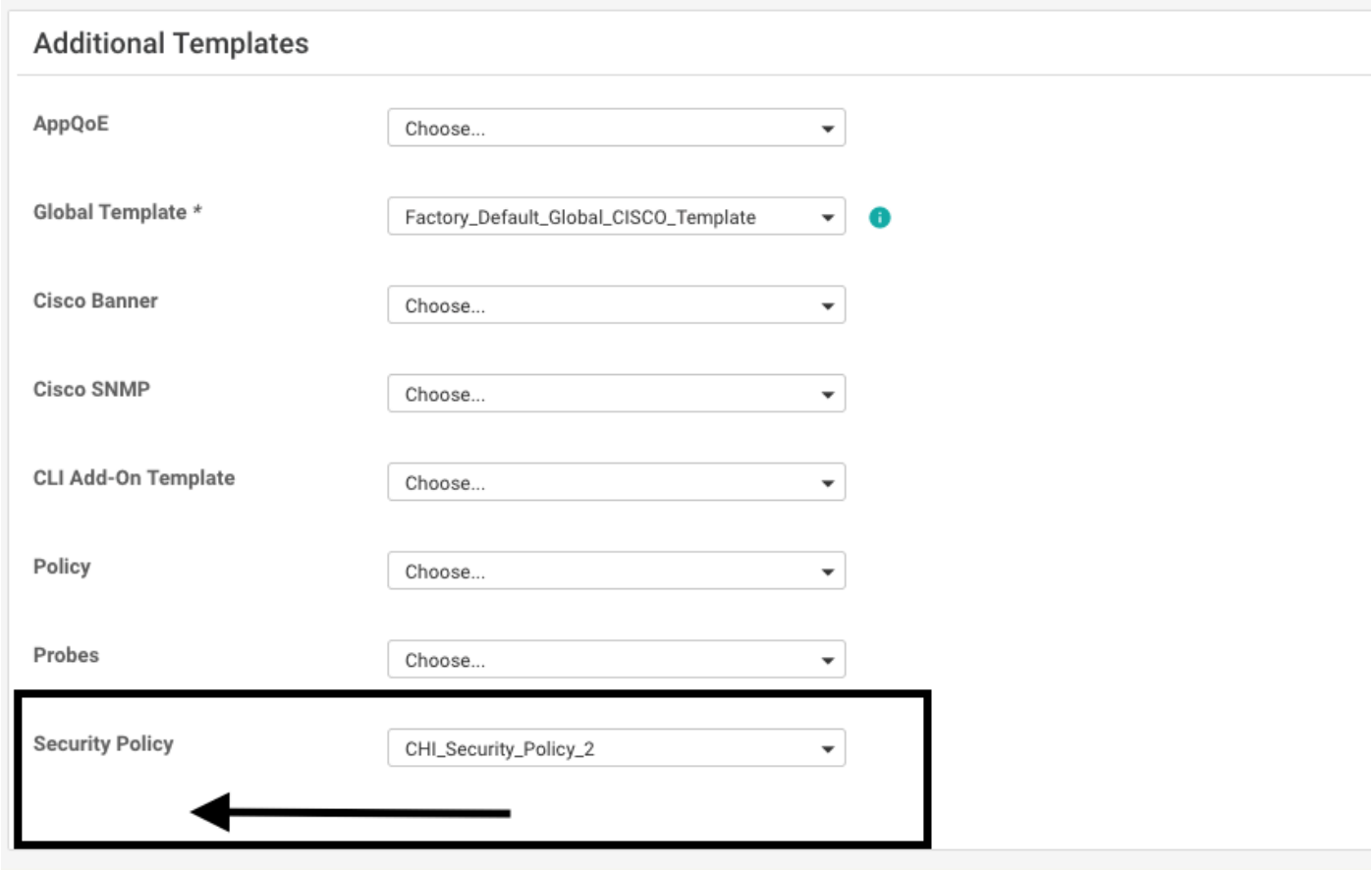
ISSUE 1. Error: Following Devices do not have Container Software Services

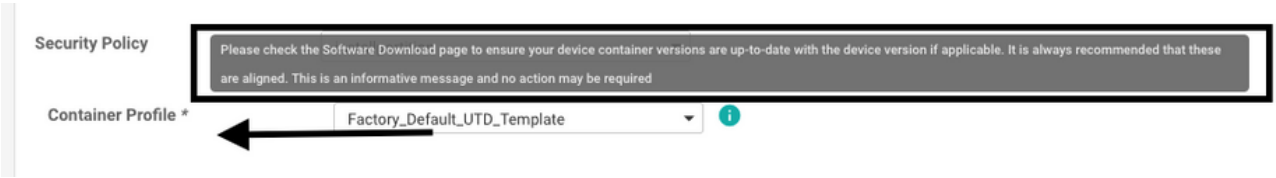
Activate the virtual image.

Navigate to **maintenance > software > activate**

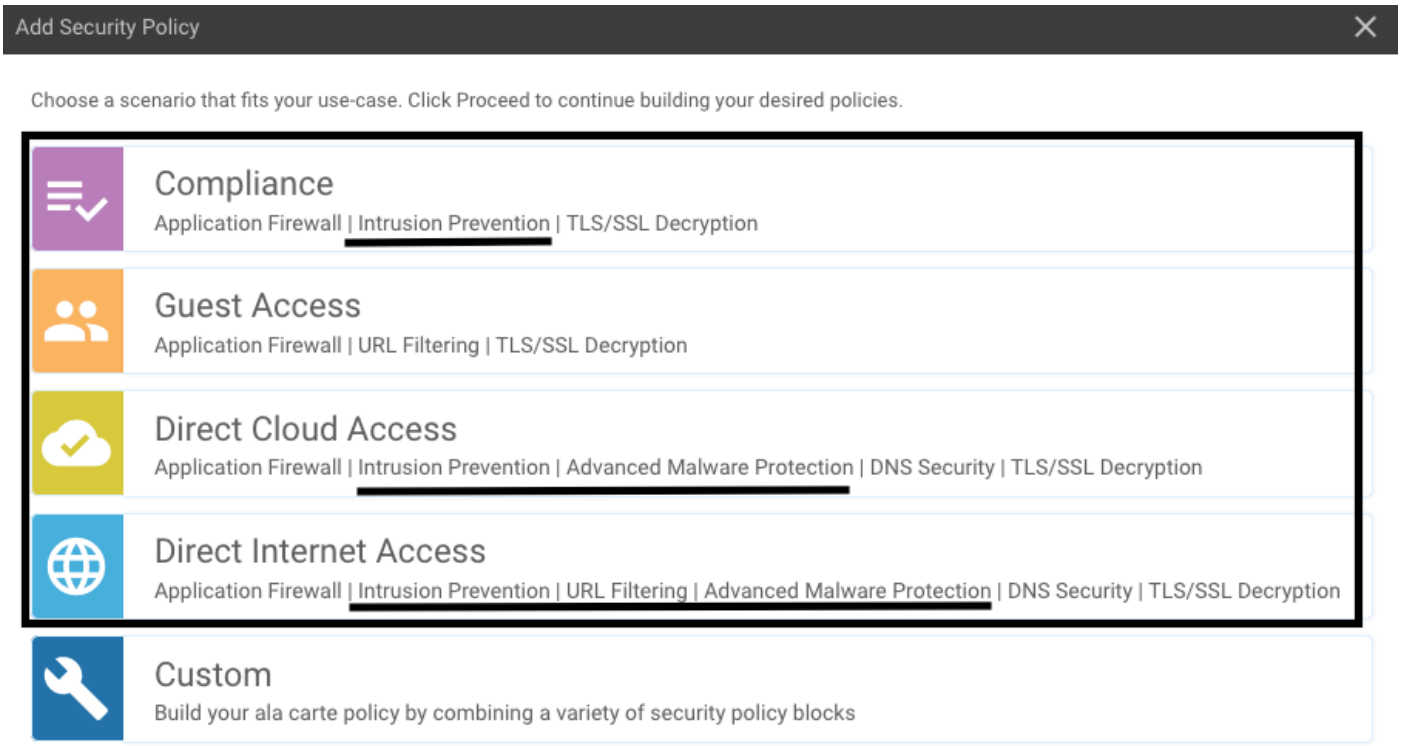


The virtual image send an error: **Devices so not have container software revices**, If the Cisco Edge router selected does not have a security policy with the container profile sub-template.





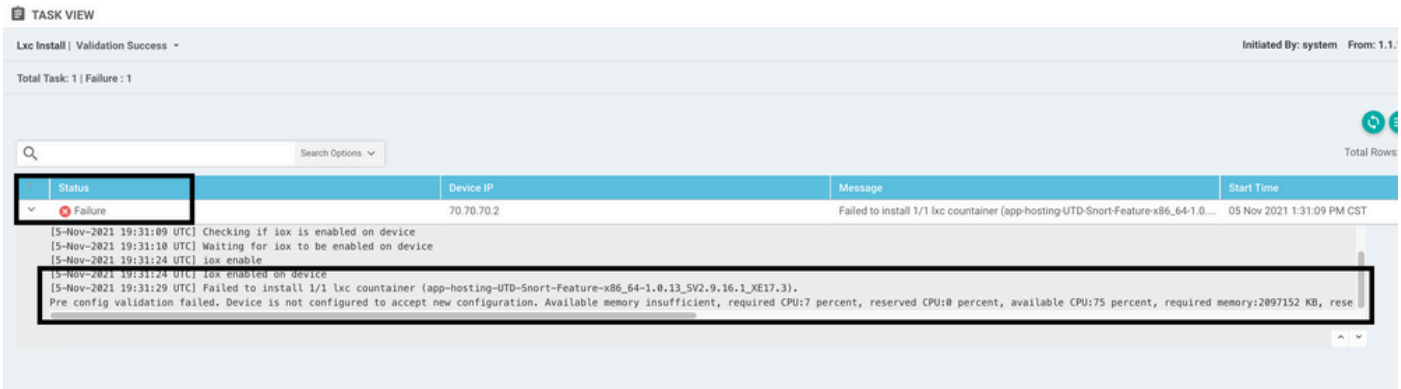
This template is automatically added if you use a Security Policy that includes security features such as Intrusion Prevention System (IPS), Intrusion Detection System (IDS), URL Filtering (URL-F), and Advanced Malware Protection (AMP) that needs UTD package. Not all the Security features available needs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



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.



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#
```

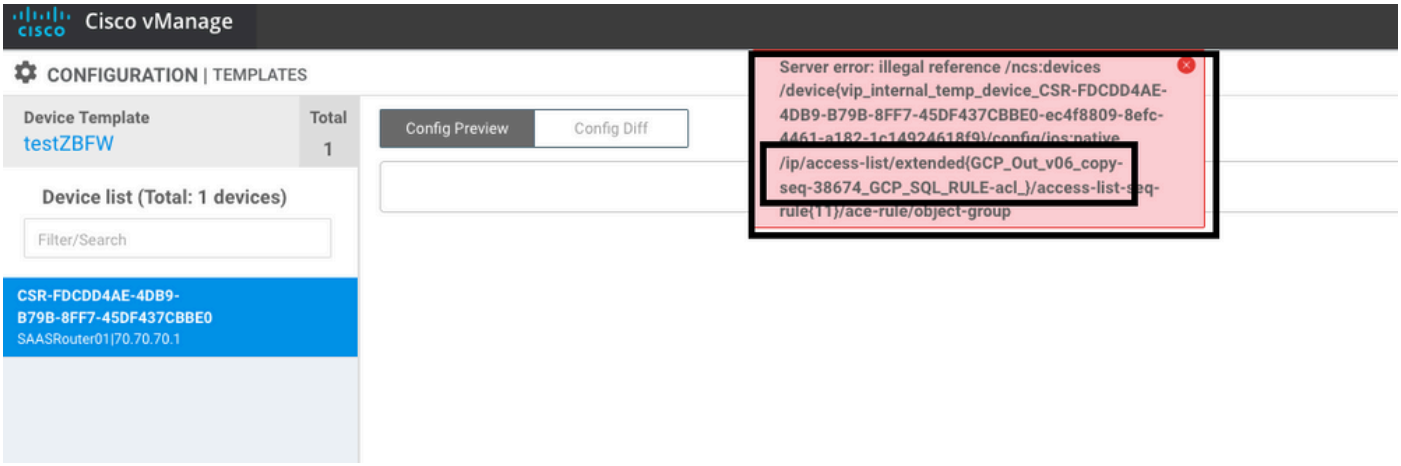
```
show sdwan system status
```

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

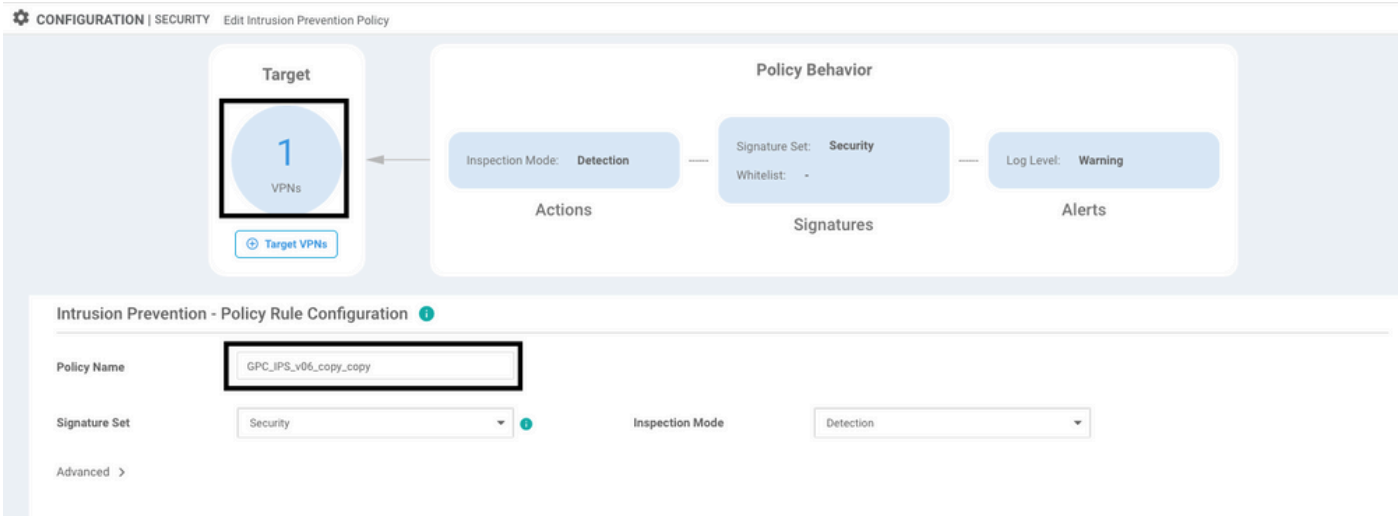
Note Sufficient free memory must be available to install UTD. If the installed DRAM is adequate but installation is still failing due to lack of memory, check current usage in **show processes memory platform sorted**

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.



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.



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