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)
<u>Configure</u>
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
<u>Verify</u>
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
<u>Video</u>
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.

Downloads Home / Routers / Software-Defined WAN (SD-WAN) /	XE SD-WAN Routers	
Cisco Interfaces and Modules	Meraki vMX	ASR 1000 Series IOS XE SD-WAN
Cloud and Systems Management	SD-WAN	CSR 1000V Series IOS XE SD-WAN
Collaboration Endpoints	XE SD-WAN Routers	ISR 1000 Series IOS XE SD-WAN
Conferencing	vEdge Router	ISR 4000 Series IOS XE SD-WAN
Connected Safety and Security		
Contact Center		
Data Center Analytics		
Hyperconverged Infrastructure		
IOS and NX-OS Software		
Optical Networking		
Routers		

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.

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	

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.

Downloads Home / Routers / Software-Def	fined WAN	I (SD-WAN) / XE SD-WAN Routers / ISR 4000 Series IOS XE SD-WAN / IOS	XE SD-WAN Software- 16	.12.5(MD)	
C Search Expand All Collapse All Suggested Release	~	ISR 4000 Series IOS XE SD-WAN Release 16.12.5 MD A My Notifications	Related Links an Release Notes for 19.2 Release Notes for 16.1	d Documentation 2.4 12.5	
Latest Release	~	File Information	Release Date	Size	
16.12.5(MD) 🔿 All Release	~	Cisco ISR 4200 Series IOS XE SD-WAN Software isr4200-ucmk9.16.12.5.SPA.bin Advisories 😭	29-Jan-2021	482.84 MB	±∵
16 Deferred Release	> ~	Cisco ISR 4300 Series IOS XE SD-WAN Software isr4300-ucmk9.16.12.5.SPA.bin Advisories 😭	29-Jan-2021	557.83 MB	±₩∎
16	>	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**.



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

Software Download

ads Home	
XE In-Service Software Upgrade (ISSU) Matrix	
XE Patch Upgrades	
XE ROMMON Software	
XE SD-WAN Software	
XE Software	
Snort IPS Engine Software	
Snort Subscriber Signature Package	
High Bitrate (VDSL) PHY Firmware	
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 Router	s / 4000) Series Integrated Services Routers / 4221 Integrated Services Router / UTD S	inort IPS Engine Software	e- 17.7.1a
Q Search Expand All Collapse All Latest Release	~	4221 Integrated Services Router Release 17.7.1a A My Notifications	Related Links and - No related links or	nd Documentation
17.7.1a Fuji-16.9.8		File Information	Release Date	Size
16.6.7a	~	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 C*	30-Nov-2021	147.72 MB
16.6	>	UTD Engine for IOS XE secapp-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.tar	30-Nov-2021	52.51 MB
17	>	Advisories 🗗		

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.



=	cisco Cisco vManag			•		≜ © .		
8		FTWARE REPOSITORY						
	Software Images Vi	rtual Images						
÷	Upload Virtual Image	ge 👻 🖸 Add Custor	n VNF Package					08
	Q		Search Options 🛩					Total Rows: 1
~	Software Version		Upload Virtual Image to vManage	Availa				
=	2.2.1	vmanage	A Do not refease the Web Beaucar or allah Web Beaucar Back butten while image is being unlanded	SDAVO	_sdavc_cont	ainer_2.2.1,	19.2.3-sd	avc.tar
			File Uploading (Total:1)					
			secano-utd 17.04.01b 1.0.9.5V2.9.16.1.XE17.4.x86.64.tar					
			Please wait. Server is Processing					

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

MAINTENANCE SOFTWARE REPOSITORY		Virtual image uploaded successfully
Software Images Virtual Images		
Opload Virtual Image ● Add Custom VNF	Package	
Q	Search Options 🗸	

cisco vManage								• 0	l u	* 2	🥑 iai	estrad 👻
MAINTENANCE SOFT	WARE REPOSITORY											
Software Images Virtu	al Images											
 Upload Virtual Image 	Add Custom VNF	Package										00
Q		Search Options 🗸									Tota	al Rows: 8
Software Version	Software Location	Network Function Type	Image Type	Architecture	Version Type Name	Vendor	Available Files			Updated	Dn	
1.0.16_SV2.9.16.1_XE17.3	vmanage	App-Hosting	Lxc	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Fea	iture-x86_64_1.0	0.16	05 Nov 21	021 2:39:19 PM	
1.0.13_SV2.9.16.1_XE17.3	vmanage	App-Hosting	Lxc	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Fea	iture-x86_64_1.0).13	05 Nov 21	021 11:31:22 A.	
1.0.12_SV2.9.16.1_XE17.4	vmanage	App-Hosting	Lxc	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Fea	iture-x86_64_1.0	0.12	05 Nov 21	021 3:51:20 PM	l
1.0.12_SV2.9.13.0_XE16	vmanage	App-Hosting	Lxc	aarch64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Fea	iture-aarch64_1.	0.12	24 Jul 20	20 10:50:24 AM	A
1.0.12_SV2.9.13.0_XE16	vmanage	App-Hosting	Lxc	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Fea	iture-x86_64_1.0	0.12	24 Jul 20	20 10:50:17 AM	A
1.0.10_SV2.9.13.0_XE17.3	vmanage	App-Hosting	Lxc	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Fea	iture-x86_64_1.0	0.10	16 Jan 20	21 9:40:36 PM	
1.0.10_SV2.9.13.0_XE16	vmanage	App-Hosting	Lxc	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Fea	ture-x86_64_1.0	0.10	18 May 2	020 10:10:22 A	
1.0.10_SV2.9.13.0_XE16	vmanage	App-Hosting	Lxc	aarch64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Fea	iture-aarch64_1.	0.10	06 Feb 20	20 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 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	1
	263	app-vnic gatewayl virtualportgroup 1 guest-interface 1
	264	guest-ipaddress 192.0.2.2 netmask 255.255.255.252
	265	4
	266	start
	267	4
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	1
	278	utd global
	279	
	280	1
	281	policy
	282	no app-visibility
	283	no flow-visibility
	284	no implicit-acl-logging
	285	log-frequency 1000
	286	1

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 F	Push Feature Template Configuration 🖉 Validation Success 👻								
Total T	Total Task: 1 Done - Scheduled : 1								
Q				Search Options 🗸					
2	Status		Message		Chassis Number	Device Model	Hostname	System IP	Site ID
>	Done - Scheduled		Device needs to	o 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.

	 ▲ ▲	admin 🛨
	Tasks	×
	Active (1) Completed (29)	
	Q	~
	Sort by Start Time 🖨	()
	Last Updated: 05 Nov 2021 11:35:18 am	
te	Lxc Install (Total 1) In progress: 1	
	Start: 05 Nov 2021 11:34:45 am By: system	

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.

TASK VIEW						
Lxc Install Validation Success *			Initiated By: system From: 1.1.1.9			
Total Task: 1 Success : 1						
٩	search Options 🗸		🙂 🖨 Total Rows: 1			
> Status	Device IP	Message	Start Time			
Y 🔮 Success	70.70.70.1	Done - Lxc Install	05 Nov 2021 12:06:03 PM CST			
15-4009-2021 18180:83 UTC Total number of fontainer apps to be installed: 1. Container apps to be installed are following: [app-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE17.3] [5-4009-2021 18:06:03 UTC] Started 1/1 Lx countainer (app-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE17.3) installation [5-409-2021 18:06:03 UTC] Onecking if Lox is emabled on device [5-409-2021 18:06:04 UTC Onecking if Lox is emabled on device [5-409-2021 18:06:04 UTC Container app image: app-hosting_UTD-Snort-Feature-x86_64_1.0.13_SV2.9.16.1_XE17.3_secapp-utd.17.03.03.1.0.13_SV2.9.16.1_XE17.3_x86_64.tar [5-409-2021 18:06:02 UTC Container on Instance: 4, Color: Diz-Internet [5-409-2021 18:06:02 UTC Connection Instance: 4, August 2000 Container (app-hosting_UTD-Snort-Feature-x86_64_1.0.13_SV2.9.16.1_XE17.3_secapp-utd.17.03.03.1.0.13_S						
L			- ×			

Verify

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

Navigate to **Configuration > Devices**

CONFIGURATION DEVICES								
WAN Edge List Controllers Unclaimed WAN Edges								
(] Change Mode 👻 Upload WAN Edge List 🗹 Export Bootstrap Configuration 🖾 Sync Smart Account								
Q 70.70.70.1 × Search Options V								
Enterprise Cert Expiration Date	Subject SUDI serial #	Hostname	System IP	Site ID	Mode	Assigned Template	Device Status	Validity
NA	NA	SAASRouter01	70.70.70.1	70	vManage	testZBFW	In Sync	valid

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

_____ 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 0wner : ioxm : RUNNING State <<<<<<<<< Application : LXC Туре Name : UTD-Snort-Feature Version : 1.0.12_SV2.9.16.1_XE17.4 <<<<<<<< Description : Unified Threat Defense Path : /bootflash/.UTD_IMAGES, : /bootflash/.UTD_IMAGES/iox-utd_1.0.12_SV2.9.16.1_XE17.4.tar URL Path Activated profile name : cloud-low Resource reservation : 2048 MB Memory 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 : Cloud-Low Profile System memory : Usage : 20.10 % Status : Green

Number of engines : 1

Engine	Running	Health	Reason	
Engine(#1):	Yes	Green	None	
<<<<<<<	<<<<<<<	<<<<		
Overall syst				
<<<<<<<	<<<<<<<	<<<		
.				
Signature up	date status ======	: ==		
Current sign Last update Last success	ature packa status: Suc ful update	ge version cessful time: Wed	: 29130.156.s Nov 25 07:27:3	35 2020 EI
<<<<<<<	<<<<<<			
Last failed Last failed Next update Current stat	update time update reas scheduled a us: Idle	: None on: None t: None		
Verify the fea	tures enable	d use the ne	ext command:	
<#root>				
Router02#				
show platfor	m hardware	qfp active	feature utd c	onfig
Global confi NAT64: dis Drop pkts: Multi-tena Data plane TLS Decryp Divert con SN threads CFT inst_i Max flows: SN Health:	guration abled disabled ncy: enable initialize tion Policy troller mod : 12 d 0 feat id 55000 channel: T channel: S	d d: yes : disabled e: enabled 2 fo id 2 hreat Defe ervice : D	chunk id 13 nse : Green own	
Context Id	: O, Name:	Global dom	ain Security (Context
Ctx Flags Engi Stat SN R Thre Doma	: (Ox1c7000 ne: Standar e edirect Mod at-inspecti in Filterin	1) d : Enable e : Fail-o on: Enable g : Not En	d pen, Divert d, Mode: IPS abled	

EDT

```
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**

	E							
WAN Edge Controller vManage								
1 Rows Selected 💿 Upgrade 💿 Up	ograde Virtual Image 💿 Activat	te Virtual Image 📑 Delete Vir	tual Image _ ල .	Activate 👔 Dele	te Available Software	🛷 Set Default Ve	ersion	000
Device Group	0.70.70.1 ×	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-B79B-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 Im Following devic Click 'Skip Devic • (SAASRo	rage ces do not have container softwar ces' to continue activate image. outer01)) services.		Skip Devices	Cancel		

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 Templa	tes	
AppQoE	Choose	•
Global Template *	Factory_Default_Global_CISCO_Template	• 0
Cisco Banner	Choose	•
Cisco SNMP	Choose	•
CLI Add-On Template	Choose	¥
Policy	Choose	•
Probes	Choose	•
Security Policy	CHI_Security_Policy_2	•
-		
Security Policy Please clare align	teck the Software Download page to ensure your device container versions are up-to-date w ed. This is an informative message and no action may be required	with the device version if applicable. It is always recommended that these
Container Profile *	Factory_Default_UTD_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.

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



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			
			00
Q. Search Options V			Total Rows
> Status	Device IP	Message	Start Time
Y S Failure	70.70.70.2	Failed to install 1/1 lxc countainer (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 de [5-Nov-2021 19:31:10 UTC] Waiting for iox to be enabled on [5-Nov-2021 19:31:24 UTC] iox enable	vice device		
[5-Nov-2021 19:31:24 UIC] lox enabled on device [5-Nov-2021 19:31:29 UIC] Failed to install 1/1 lxc counta Pre config validation failed. Device is not configured to end to the second secon	iner (app-hosting-UTD-Snort-Feature-x86_64-1.0.13_5V2.9.16.1_XE17.3). accept new configuration. Available memory insufficient, required CPU:7	percent, reserved CPU:0 percent, available CPU:75 percent, required	memory:2097152 KB, rese
			A 9

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

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.

CONFIGURATION SECURITY Edit Intrusion Prevention Policy							
Target		Policy Behavior					
1 VPNs	Inspection Mode: Detection	Signature Set: Security Whitelist: -	Log Level: Warning				
⊕ Target VPNs	Actions	Signatures	Alerts				
Intrusion Prevention - Policy Rule Configuration 0							
Policy Name GPC_IPS_v06_copy_copy							
Signature Set Security	▼ 0 Ins	pection Mode Detection	•				
Advanced >							

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 statu	IS			
UTD engine standard is not ena	ıbled			
ISR01#show sdwan virtual-appli	cation u	ıtd		
VERSION		ACTIVE	PREVIOUS	TIMESTAMP
1.0.16_SV2.9.16.1_XE17.3	true	tru	e	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
- <u>Cisco SD-WAN Security Configuration Guide, Cisco IOS XE Release</u>
- <u>Technical Support & Documentation Cisco Systems</u>