

在cEdge路由器上安裝UTD安全虛擬映像

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[執行Cisco IOS XE SD-WAN軟體\(16.x\)的路由器](#)

[執行Cisco IOS XE軟體\(17.x\)的路由器](#)

[設定](#)

[步驟 1.上傳虛擬映像](#)

[步驟 2.將安全策略和容器配置檔案子模板新增到裝置模板](#)

[步驟 3.使用安全策略和容器配置檔案更新或附加裝置模板](#)

[驗證](#)

[常見問題](#)

[問題1.錯誤：以下裝置沒有容器軟體服務](#)

[問題2.可用記憶體不足](#)

[問題3.非法引用](#)

[第四期。UTD已安裝且活動，但未啟用](#)

[影片](#)

[相關資訊](#)

簡介

本檔案介紹如何安裝整合威脅防禦(UTD)安全虛擬映像，以在Cisco IOS® XE SD-WAN裝置上啟用安全功能。

必要條件

- 使用這些功能之前，請將相關的安全虛擬映像上傳到vManage儲存庫。
- Cisco Edge路由器必須處於vmanage模式，且必須預先連線模板。
- 為入侵防禦系統(IPS)、入侵檢測系統(IDS)、URL過濾(URL-F)或高級惡意軟體防護(AMP)過濾建立安全策略模板。

需求

- 4000整合式服務路由器Cisco IOS XE SD-WAN(ISR4k)
- 1000整合式服務路由器Cisco IOS XE SD-WAN(ISR1k)
- 1000v雲端服務路由器(CSR1kv),
- 1000v整合式服務路由器(ISRv)
- 支援8 GB DRAM的Cisco Edge平台。

採用元件

- Cisco UTD虛擬映像
- vManage控制器
- 思科邊緣路由器，帶有與控制器的控制連線。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco UTD映像需要在要安裝的裝置模板上安裝安全策略，並且在Cisco Edge路由器上啟用安全功能，例如入侵防禦系統(IPS)、入侵檢測系統(IDS)、URL過濾(URL-F)和高級惡意軟體防護(AMP)。

從軟體Cisco下載Cisco UTD Snort IP引擎軟體

使用當前Cisco IOS XE版本支援的Cisco UTD虛擬映像正規表示式。使用命令show utd engine standard version驗證推薦的和支援的UTD映像。

```
<#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$
```

 注意下載映像的路徑取決於路由器是執行Cisco IOS XE SD-WAN軟體(16.x)還是通用Cisco IOS XE軟體(17.x)。

執行Cisco IOS XE SD-WAN軟體(16.x)的路由器

獲取Cisco UTD Snort IPS引擎軟體的路徑為路由器/軟體定義WAN(SD-WAN)/XE SD-WAN路由器/和系列整合路由器。

[Downloads Home](#) / [Routers](#) / [Software-Defined WAN \(SD-WAN\)](#)

The screenshot shows a navigation menu with three columns. The first column lists various Cisco product categories, with 'Routers' highlighted in blue. The second column lists router types, with 'Software-Defined WAN (SD-WAN)' highlighted in blue. The third column lists specific router models, with 'XE SD-WAN Routers' highlighted in blue.

選擇思科邊緣路由器的型號型別。



注意Series Aggregation Services Routers(ASR)不適用於UTD功能。

[Downloads Home](#) / [Routers](#) / [Software-Defined WAN \(SD-WAN\)](#) / [XE SD-WAN Routers](#)

The screenshot shows the 'XE SD-WAN Routers' page. The left navigation menu has 'Routers' highlighted. The main content area shows a list of router models: Meraki vMX, SD-WAN, XE SD-WAN Routers (highlighted in blue), and vEdge Router. A dashed box highlights the 'ASR 1000 Series IOS XE SD-WAN' model, which is not selected.

選擇型別路由器型號後，選擇Cisco IOS XE SD-WAN軟體選項，以獲取16.x版Cisco Edge的UTD包

。

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

The screenshot shows the 'ISR 4000 Series IOS XE SD-WAN' page. The main content area has the heading 'Select a Software Type' and three links: 'IOS XE In-Service Software Upgrade (ISSU) Matrix', 'IOS XE SD-WAN Software' (highlighted in blue), and 'IOS XE Software'.



注意：為Cisco Edge路由器選擇Cisco UTD虛擬映像（適用於16.x代碼）的下載路徑還顯示Cisco IOS XE軟體選項。這是只為17.x選擇Cisco Edge升級代碼的路徑，但找不到版本17.x的UTD虛擬映像。17.x和最新版本上的Cisco統一常規Cisco IOS XE和Cisco IOS XE SD-WAN代碼，因此獲取17.x的Cisco UTD虛擬映像的路徑與常規Cisco IOS XE代碼相同。

選擇當前版本的Cisco Edge，然後下載該版本的UTD軟體包。

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	Download Buy
Cisco ISR 4300 Series IOS XE SD-WAN Software isr4300-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	557.83 MB	Download Buy
Cisco ISR 4400 Series IOS XE SD-WAN Software isr4400-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	621.88 MB	Download Buy
Cisco ISR 4400v2 Series IOS XE SD-WAN Software isr4400v2-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	623.49 MB	Download Buy
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	Download Buy

執行Cisco IOS XE軟體(17.x)的路由器

Cisco IOS XE版本17.2.1r和最新版本使用universalk9映像，在Cisco IOS XE裝置上部署Cisco IOS XE SD-WAN和Cisco IOS XE。

UTD Snort IPS引擎軟體位於Routers > Branch Routers > Series Integrated Router中。

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

選擇路由器的型號型別後，請選擇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](#)

選擇路由器的當前版本，並為選定的版本下載UTD軟體包。

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

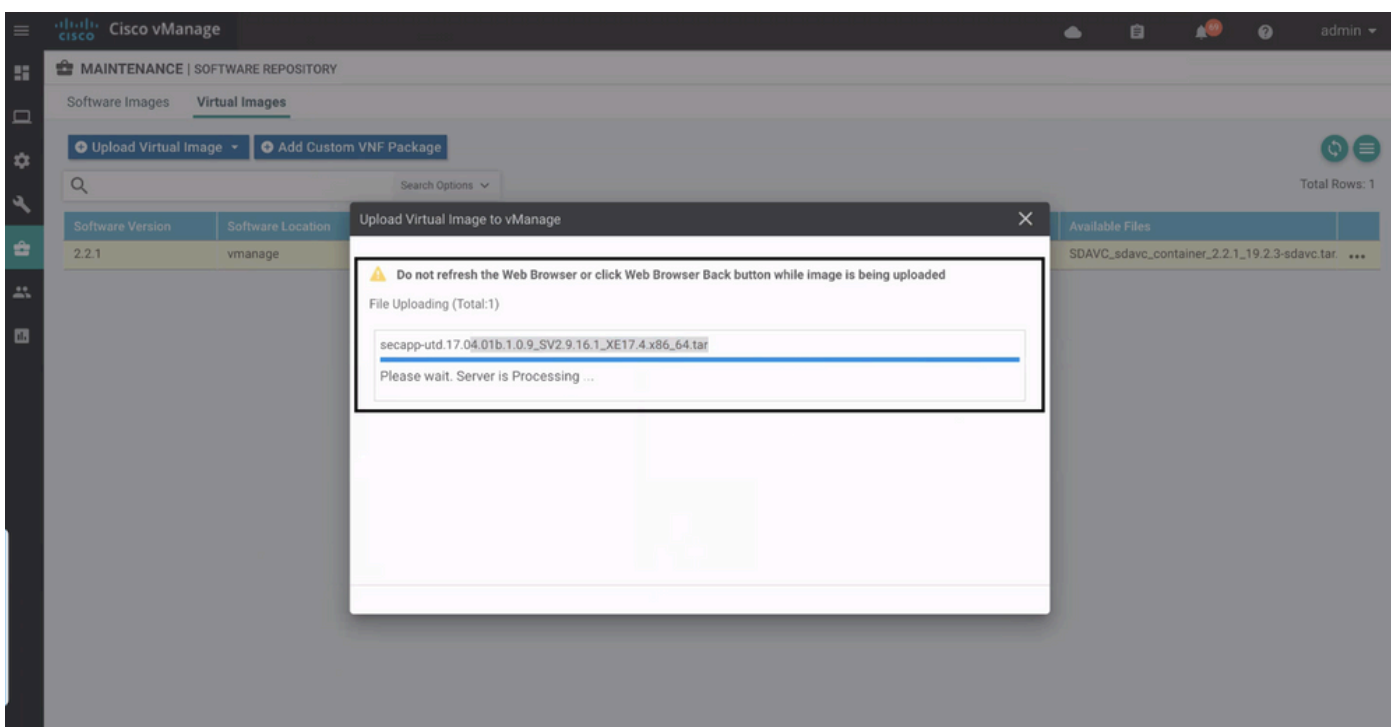
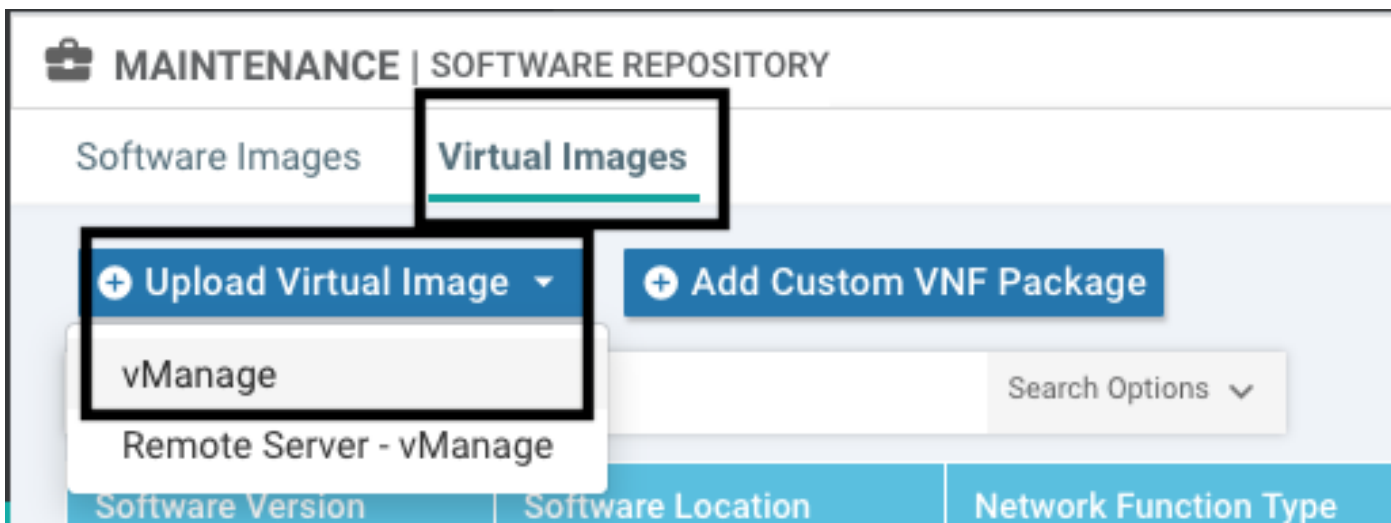
註：運行Cisco IOS XE軟體而非Viptela代碼的Cisco ISR1100X系列路由器（Cisco Nutella路由器SR1100X-4G/6G）基於x86_x64。為ISR4K發佈的Cisco UTD虛擬映像可以在這些映像上運行。您可以在Nutella路由器上安裝當前Cisco IOS XE SD-WAN版本支援的同一Cisco UTD映像代碼版本regex。使用命令show utd engine standard version驗證建議且受支援的regex Cisco UTD映像。

設定

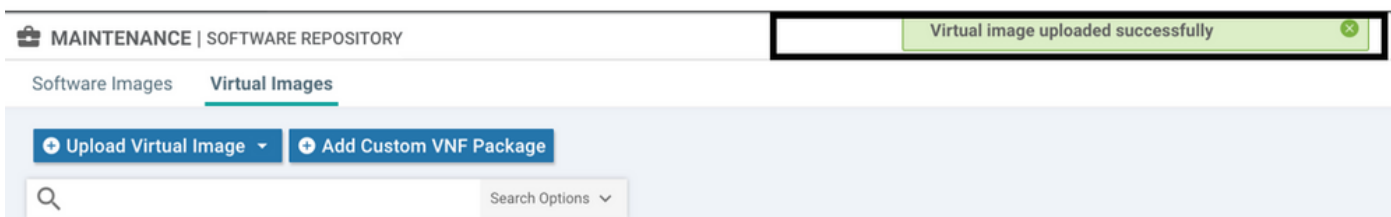
步驟 1.上傳虛擬映像

確保您的虛擬映像與Cisco Edge上當前的Cisco IOS XE SD-WAN代碼相匹配，然後將其上傳到vmanage儲存庫。

導航到維護>軟體儲存庫>虛擬映像>上傳虛擬映像> vManage。



成功上載Cisco UTD虛擬映像後，請仔細檢查其是否位於儲存庫中。



Cisco vManage MAINTENANCE | SOFTWARE REPOSITORY

Software Images Virtual Images

Upload Virtual Image Add Custom VNF Package

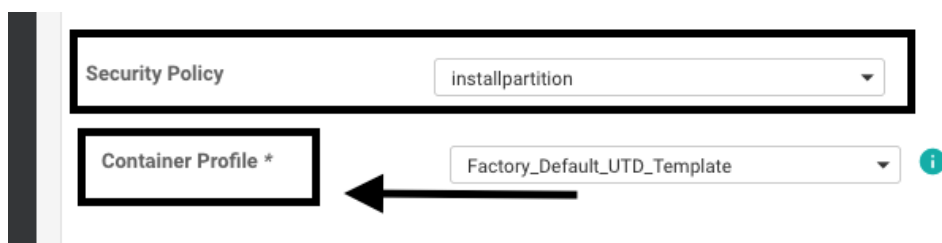
Search Options

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 ...

步驟 2.將安全策略和容器配置檔案子模板新增到裝置模板

將之前建立的安全策略新增到裝置模板。安全策略必須具有IPS/IDS、URL-F或AMP過濾策略，才能將其新增到裝置模板中。自動開啟容器配置檔案。使用預設容器配置檔案或在需要時對其進行修改。



步驟 3.使用安全策略和容器配置檔案更新或附加裝置模板

將模板更新或附加到思科邊緣路由器。請注意，在config diff中，已配置功能IPS/IDS、URL-F或AMP過濾的應用託管配置和UTD引擎。

```

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 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 !

```

由於vmanage注意到應用的配置具有UTD引擎功能，因此模板狀態更改為Done-scheduled，因此vmanage確定Cisco Edge需要安裝虛擬映像才能使用UTD安全功能。

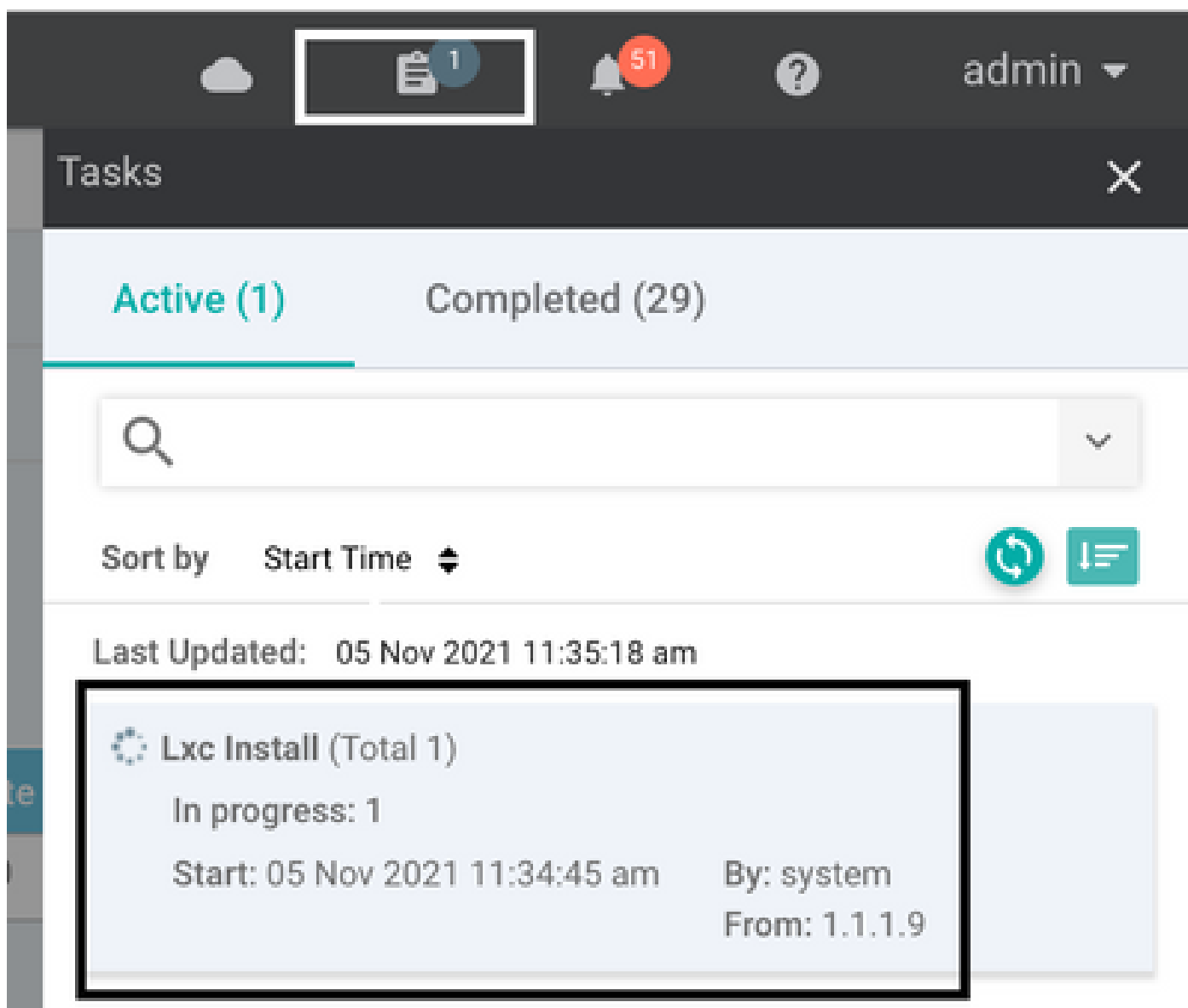


Push Feature Template Configuration | Validation Success

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

將模板移動到計畫狀態後，任務選單中將顯示一個正在進行的新任務。新任務是Lxc安裝，這意味著vmanage在推送新配置之前自動開始將虛擬映像安裝到Cisco Edge。



Tasks

Active (1) Completed (29)

Sort by Start Time

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

安裝LX容器後，vManage會使用UTD功能推送計畫前配置。由於之前已計畫配置，因此沒有此任務的新任務。


```
App id                               State
-----
utd                                  RUNNING
<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

下一個命令彙總了先前的命令並顯示當前狀態和版本：

```
<#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 命令顯示UTD引擎的健康狀況以及獲取特徵碼更新的清單時間。

```
<#root>
```

```
Router02#
```

```
show utd engine standard status
```

```
Engine version   : 1.0.6_SV2.9.13.0_XE17.2
Profile          : Cloud-Low
```


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

常見問題

問題1.錯誤：以下裝置沒有容器軟體服務

啟用虛擬映像。

導航到維護>軟體>啟用

The screenshot shows a 'MAINTENANCE | SOFTWARE UPGRADE' interface. At the top, there are tabs for 'WAN Edge', 'Controller', and 'vManage'. Below the tabs, there is a search bar and several action buttons: 'Upgrade', 'Upgrade Virtual Image', 'Activate Virtual Image', 'Delete Virtual Image', 'Activate', 'Delete Available Software', and 'Set Default Version'. A table lists devices with columns for Hostname, System IP, Chassis Number, Site ID, Device Model, Reachability, Current Version, Available Versions, Default Version, Available Services, and Up Since. One device, 'SAASRouter01', is highlighted. A dialog box titled 'Activate Virtual Image' is open, displaying an error message: 'Following devices do not have container software services. Click 'Skip Devices' to continue activate image.' The device '(SAASRouter01)' is listed in the dialog. The dialog has 'Skip Devices' and 'Cancel' buttons.

虛擬映像傳送錯誤： Devices so not have container software refs (裝置沒有容器軟體版本)。如果所選的Cisco Edge路由器沒有容器配置檔案子模板的安全策略。

Additional Templates

AppQoS	Choose...
Global Template *	Factory_Default_Global_CISCO_Template i
Cisco Banner	Choose...
Cisco SNMP	Choose...
CLI Add-On Template	Choose...
Policy	Choose...
Probes	Choose...
Security Policy	CHI_Security_Policy_2

Security Policy	<div style="border: 1px solid black; padding: 5px;"><p>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</p></div>
Container Profile *	Factory_Default_UTD_Template i

如果您使用的安全策略包括需要UTD軟體包的安全功能(如入侵防禦系統(IPS)、入侵檢測系統(IDS)、URL過濾(URL-F)和高級惡意軟體防護(AMP))，則會自動新增此模板。並非所有可用的安全功能都需要UTD引擎，例如簡單ZBFW功能。

✕

Add Security Policy

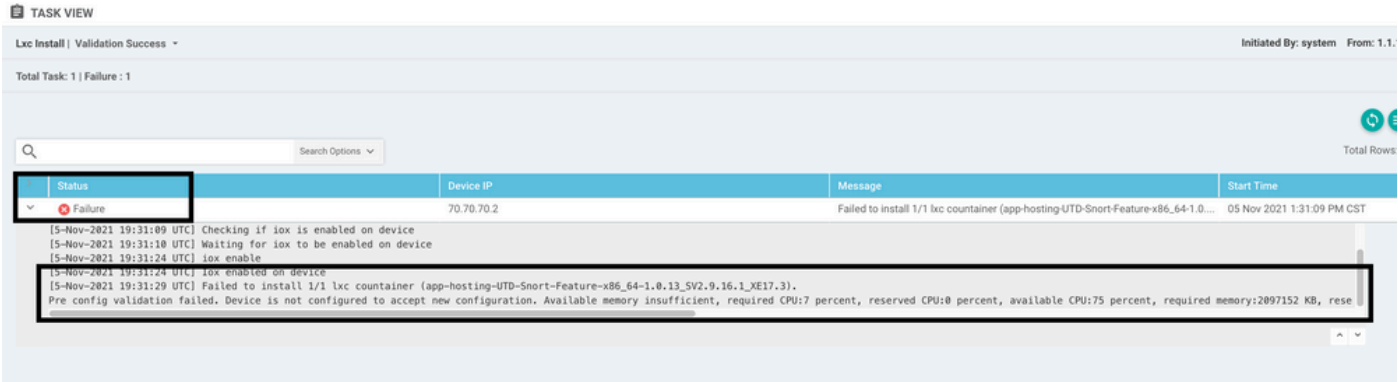
Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

- 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

使用容器配置檔案子模板推送模板後，vmanage將自動安裝虛擬映像。

問題2. 可用記憶體不足

確保Cisco Edge路由器具有8 GB DRAM記憶體，如果沒有，則Lxc安裝過程會將裝置配置為接受新配置。可用記憶體不足錯誤。Cisco Edge路由器使用UTD功能的要求是至少有8 GB的DRAM。



在此案例中，CSRv只有4 GB DRAM。將記憶體升級到8GB DRAM後，安裝成功。

使用show sdwan system status輸出驗證當前的總記憶體：

```
<#root>
```

```
Router01#
```

```
show sdwan system status
```

```
Memory usage:            8107024K total,      3598816K used,      4508208K free
```

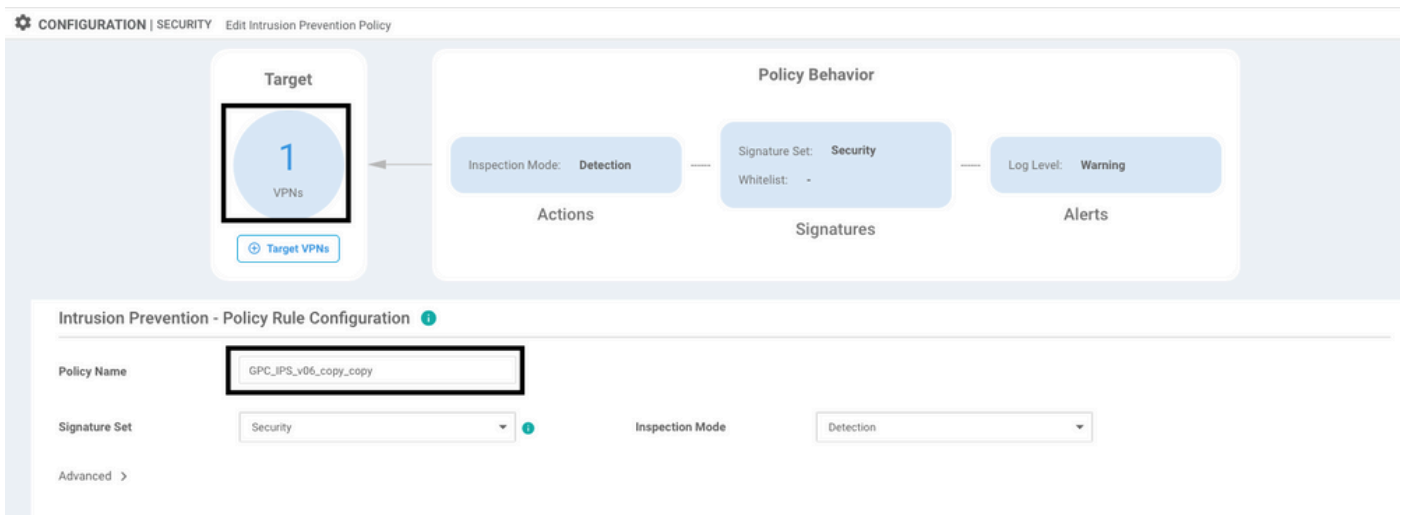
 注意：必須提供足夠的可用記憶體才能安裝UTD。如果安裝的DRAM已足夠，但由於記憶體不足而安裝仍失敗，請檢查show processes memory platform sorted中的當前使用情況

問題3.非法引用

確保已在思科邊緣路由器中配置用於任何安全策略功能的VPN/VRF，以避免安全策略序列的非法引用。



在本示例中，安全策略具有用於VPN/VRF 1的入侵防禦策略，但裝置未配置任何VRF 1。因此，vmanage會為該策略序列傳送非法引用。



配置安全策略中提到的VRF後，不會出現Illegal引用，並且已成功推送模板。

第四期。UTD已安裝且活動，但未啟用

裝置已配置安全策略，UTD已安裝並處於活動狀態，但未啟用。

此問題與問題3相關，但是vManage允許配置引用未在裝置中配置的VRF，並且策略未應用於任何

VRF。

要確定路由器是否遇到此問題，您需要看到UTD處於活動狀態。UTD未啟用消息，並且策略未引用任何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

對於解決方案，請驗證目標VPN並確保將策略應用到配置的VRF。

影片

[在cEdge路由器上安裝UTD安全虛擬映像](#)

相關資訊

- [路由器安全：路由器上的Snort IPS](#)
- [Cisco SD-WAN安全配置指南，Cisco IOS XE版本](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。