

# Installa immagine virtuale di sicurezza UTD su router cEdge

## Sommario

---

### [Introduzione](#)

### [Prerequisiti](#)

#### [Requisiti](#)

#### [Componenti usati](#)

#### [Premesse](#)

[Router che eseguono il software Cisco IOS XE SD-WAN \(16.x\)](#)

[Router con software Cisco IOS XE \(17.x\)](#)

### [Configurazione](#)

[Passaggio 1. Carica immagine virtuale](#)

[Passaggio 2. Aggiungi criterio di protezione e sottomodulo di profilo contenitore al modello di dispositivo](#)

[Passaggio 3. Aggiornare o collegare il modello di dispositivo con il criterio di protezione e il profilo del contenitore](#)

### [Verifica](#)

### [Problemi comuni](#)

[NUMERO 1. Errore: i seguenti dispositivi non dispongono di servizi software contenitore](#)

[NUMERO 2. Memoria disponibile insufficiente](#)

[NUMERO 3. Riferimento non valido](#)

[NUMERO 4. UTD installato e attivo ma non abilitato](#)

### [Video](#)

### [Informazioni correlate](#)

---

## Introduzione

Questo documento descrive come installare l'immagine virtuale di sicurezza UTD (Unified Threat Defense) per abilitare le funzionalità di sicurezza sui dispositivi Cisco IOS® XE SD-WAN.

## Prerequisiti

- Prima di utilizzare queste funzionalità, caricare l'immagine virtuale di sicurezza appropriata nel repository vManage.
- Il router Cisco Edge deve essere in modalità di gestione con il modello preallegato.
- Creare un modello di criteri di sicurezza per i filtri IPS (Intrusion Prevention System), IDS (Intrusion Detection System), URL-F (URL Filtering) o AMP (Advanced Malware Protection).

## Requisiti

- 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),
- ISRV (1000v Integrated Services Router)
- Piattaforme Cisco Edge che supportano DRAM da 8 GB.

## Componenti usati

- Immagine virtuale UTD Cisco
- vManage controller
- Router Cisco Edge con connessioni di controllo con controller.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Per installare l'immagine Cisco UTD, è necessario un criterio di sicurezza nel modello di dispositivo e le funzionalità di sicurezza abilitate, ad esempio IPS (Intrusion Prevention System), IDS (Intrusion Detection System), URL Filtering (URL-F) e AMP (Advanced Malware Protection), devono essere abilitate sui router Cisco Edge.

Scarica il software Cisco UTD Snort IP Engine dal [software Cisco](#)

Usare il regex supportato dall'immagine virtuale Cisco UTD per la versione corrente di Cisco IOS XE. Utilizzare il comando `show utd engine standard version` per convalidare l'immagine UTD consigliata e supportata.

```
<#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$
```



Nota Il percorso per il download dell'immagine dipende dal fatto che il router esegua il software Cisco IOS XE SD-WAN (16.x) o il software Cisco IOS XE universale (17.x).

---

Router che eseguono il software Cisco IOS XE SD-WAN (16.x)

Il percorso per ottenere il software Cisco UTD Snort IPS Engine è Router/ Software-Defined WAN

(SD-WAN)/ Router XE SD-WAN / e router integrati della serie.

The screenshot shows a navigation menu with the following structure:

- Downloads Home / Routers / Software-Defined WAN (SD-WAN)
- Left sidebar menu items: 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 (highlighted).
- Main menu items: 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, Software-Defined WAN (SD-WAN) (highlighted).
- Right sidebar menu items: Meraki vMX, SD-WAN, XE SD-WAN Routers (highlighted), vEdge Router.

Selezionare il tipo di modello per il router Cisco Edge.

 Nota: i router ASR (Series Aggregation Services Router) non sono disponibili per le funzionalità UTD.

The screenshot shows the navigation path: Downloads Home / Routers / Software-Defined WAN (SD-WAN) / XE SD-WAN Routers.

- Left sidebar menu items: 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 (highlighted).
- Main menu items: Meraki vMX, SD-WAN, XE SD-WAN Routers (highlighted), vEdge Router.
- Right sidebar menu items: ASR 1000 Series IOS XE SD-WAN (dashed border), CSR 1000V Series IOS XE SD-WAN, ISR 1000 Series IOS XE SD-WAN, ISR 4000 Series IOS XE SD-WAN.

Dopo aver scelto il tipo di modello di router, selezionare l'opzione software Cisco IOS XE SD-WAN per ottenere il pacchetto UTD per Cisco Edges sulla versione 16.x.

The screenshot shows the navigation path: 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](#) (highlighted)
- [IOS XE Software](#)

 Nota Il percorso di download per la scelta dell'immagine virtuale Cisco UTD per il codice 16.x per i router Cisco Edge mostra anche l'opzione software Cisco IOS XE. Questo è il percorso per scegliere i codici di aggiornamento di Cisco Edge solo per 17.x, ma non è presente l'immagine virtuale UTD per la versione 17.x. Cisco ha unificato i codici Cisco IOS XE e

 Cisco IOS XE SD-WAN regolari sulla versione 17.x e successive, quindi il percorso per ottenere l'immagine virtuale Cisco UTD per la versione 17.x è lo stesso dei normali codici Cisco IOS XE.

Scegliere la versione corrente di Cisco Edge e scaricare il pacchetto UTD per tale versione.

Downloads Home / Routers / Software-Defined WAN (SD-WAN) / XE SD-WAN Routers / ISR 4000 Series IOS XE SD-WAN / **IOS XE SD-WAN Software- 16.12.5(MD)**

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 <a href="#">Advisories</a>	29-Jan-2021	482.84 MB	  
Cisco ISR 4300 Series IOS XE SD-WAN Software isr4300-ucmk9.16.12.5.SPA.bin <a href="#">Advisories</a>	29-Jan-2021	557.83 MB	  
Cisco ISR 4400 Series IOS XE SD-WAN Software isr4400-ucmk9.16.12.5.SPA.bin <a href="#">Advisories</a>	29-Jan-2021	621.88 MB	  
Cisco ISR 4400v2 Series IOS XE SD-WAN Software isr4400v2-ucmk9.16.12.5.SPA.bin <a href="#">Advisories</a>	29-Jan-2021	623.49 MB	  
<b>UTD Engine for IOS XE SD-WAN</b> secapp-ucmk9.16.12.05.1.0.18_SV2.9.16.1_XE16.12.x86_64.tar <a href="#">Advisories</a>	29-Jan-2021	52.01 MB	  

Router con software Cisco IOS XE (17.x)

Cisco IOS XE versione 17.2.1r e la versione più recente usano l'immagine universalk9 per installare Cisco IOS XE SD-WAN e Cisco IOS XE sui dispositivi Cisco IOS XE.

Il software UTD Snort IPS Engine si trova in Router > Router per filiali > Router integrati in 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

Dopo aver scelto il tipo di modello del router, selezionare il software UTD Snort IPS Engine.

# 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](#)

Selezionare la versione corrente del router e scaricare il pacchetto UTD per la versione selezionata.

## 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 <a href="#">iosxe-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.ova</a> <a href="#">Advisories</a>	30-Nov-2021	147.72 MB
UTD Engine for IOS XE <a href="#">secapp-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.tar</a> <a href="#">Advisories</a>	30-Nov-2021	52.51 MB

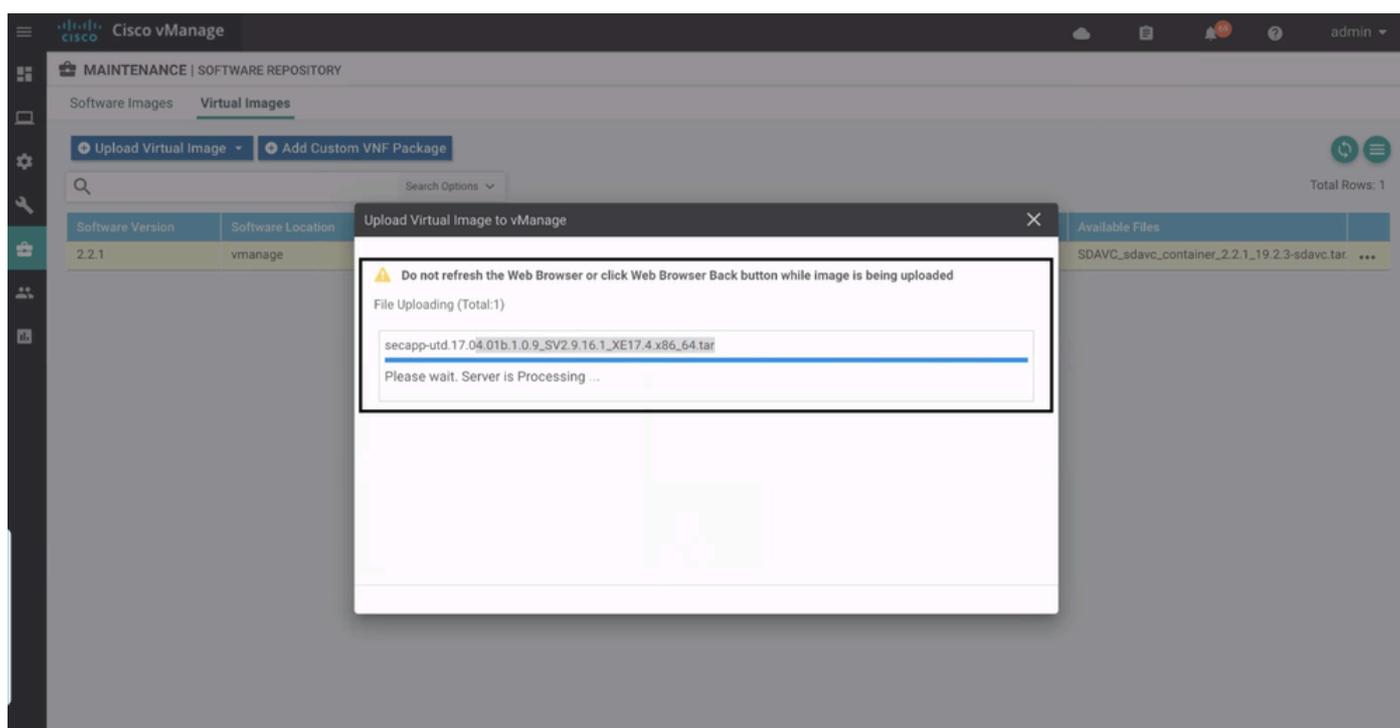
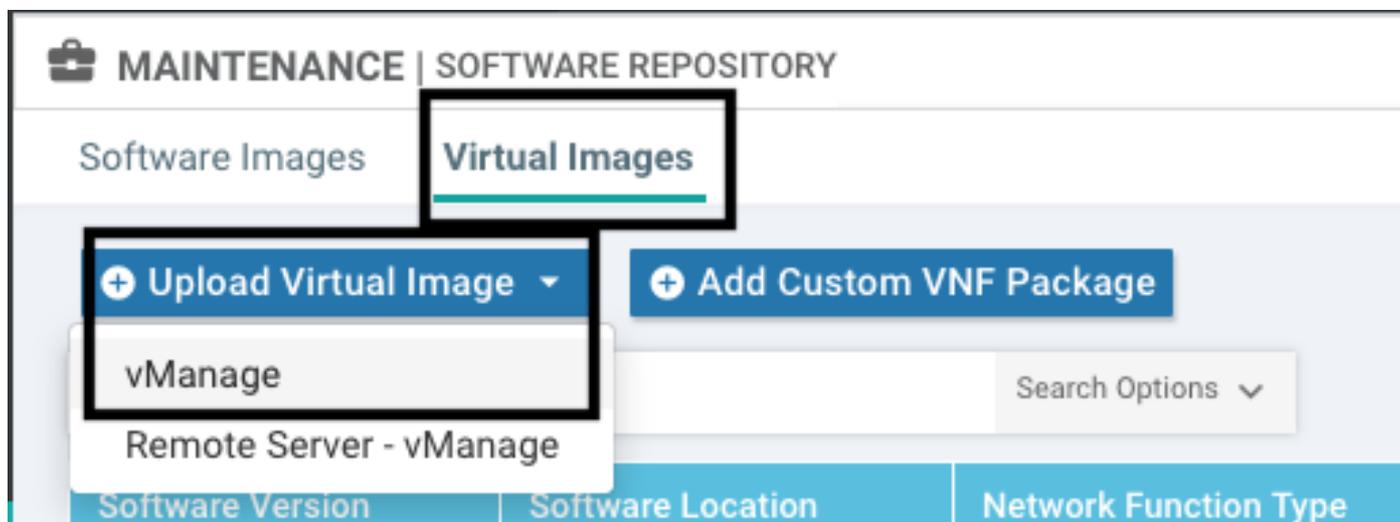
 Nota: i router Cisco serie ISR1100X (Cisco Nutella SR1100X-4G/6G) con software Cisco IOS XE anziché con codice Viptela sono basati su x86\_x64. È possibile utilizzare l'immagine virtuale UTD Cisco pubblicata per ISR4K. È possibile installare sul router Nutella la stessa versione del codice di immagine UTD Cisco supportata dal regex per la versione corrente di Cisco IOS XE SD-WAN. Utilizzare il comando `show utd engine standard version` per convalidare l'immagine UTD Cisco regex consigliata e supportata.

## Configurazione

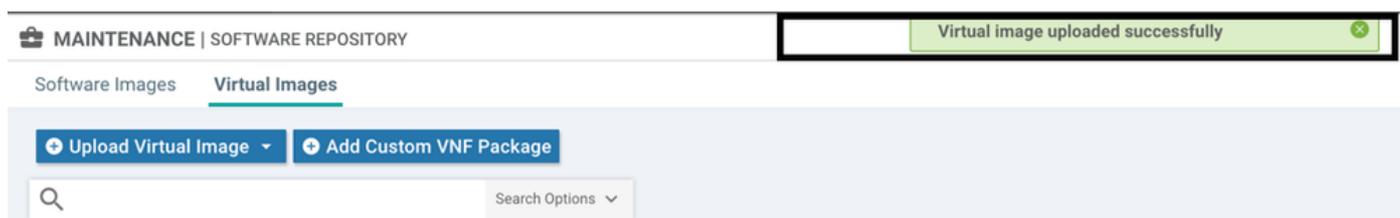
## Passaggio 1. Carica immagine virtuale

Verificare che l'immagine virtuale corrisponda al codice Cisco IOS XE SD-WAN corrente sul perimetro Cisco e caricarla in per gestire il repository.

Passare a Manutenzione > Repository software > Immagine virtuale > Carica immagine virtuale > vManage.



Una volta caricata correttamente l'immagine virtuale Cisco UTD, verificare che si trovi nel repository.



Cisco vManage MAINTENANCE | SOFTWARE REPOSITORY

Software Images Virtual Images

Upload Virtual Image Add Custom VNF Package

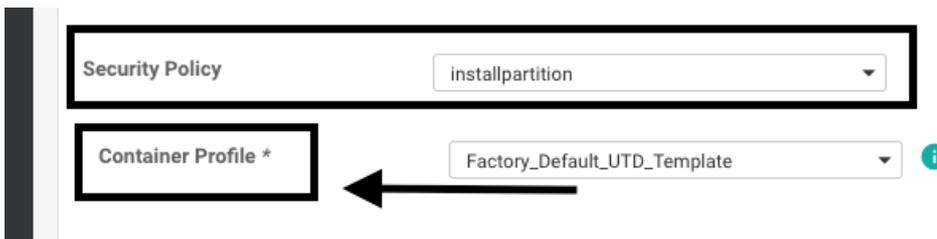
Search Options

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	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	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	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	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	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	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	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	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-aarch64_1.0.10...	06 Feb 2020 9:39:51 AM ...

## Passaggio 2. Aggiungi criterio di protezione e sottomodello di profilo contenitore al modello di dispositivo

Aggiungere il criterio di protezione creato in precedenza al modello di dispositivo. Il criterio di protezione deve includere un criterio di filtro IPS/IDS, URL-F o AMP nel modello del dispositivo. Aprire automaticamente il profilo contenitore. Utilizzare il profilo contenitore predefinito o modificarlo se necessario.



## Passaggio 3. Aggiornare o collegare il modello di dispositivo con il criterio di protezione e il profilo del contenitore

Aggiornare o collegare il modello al router Cisco Edge. Notare sulle differenze di configurazione che è configurata la configurazione di hosting dell'app e il motore UTD per la funzionalità IPS/IDS, URL-F o filtro AMP.

```

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 !

```

Lo stato del modello viene modificato in Fatto-pianificato perché il gestore ha notato che la configurazione applicata ha funzionalità del motore UTD, quindi il gestore determina che il Cisco Edge deve installare l'immagine virtuale per usare le funzionalità di sicurezza UTD.

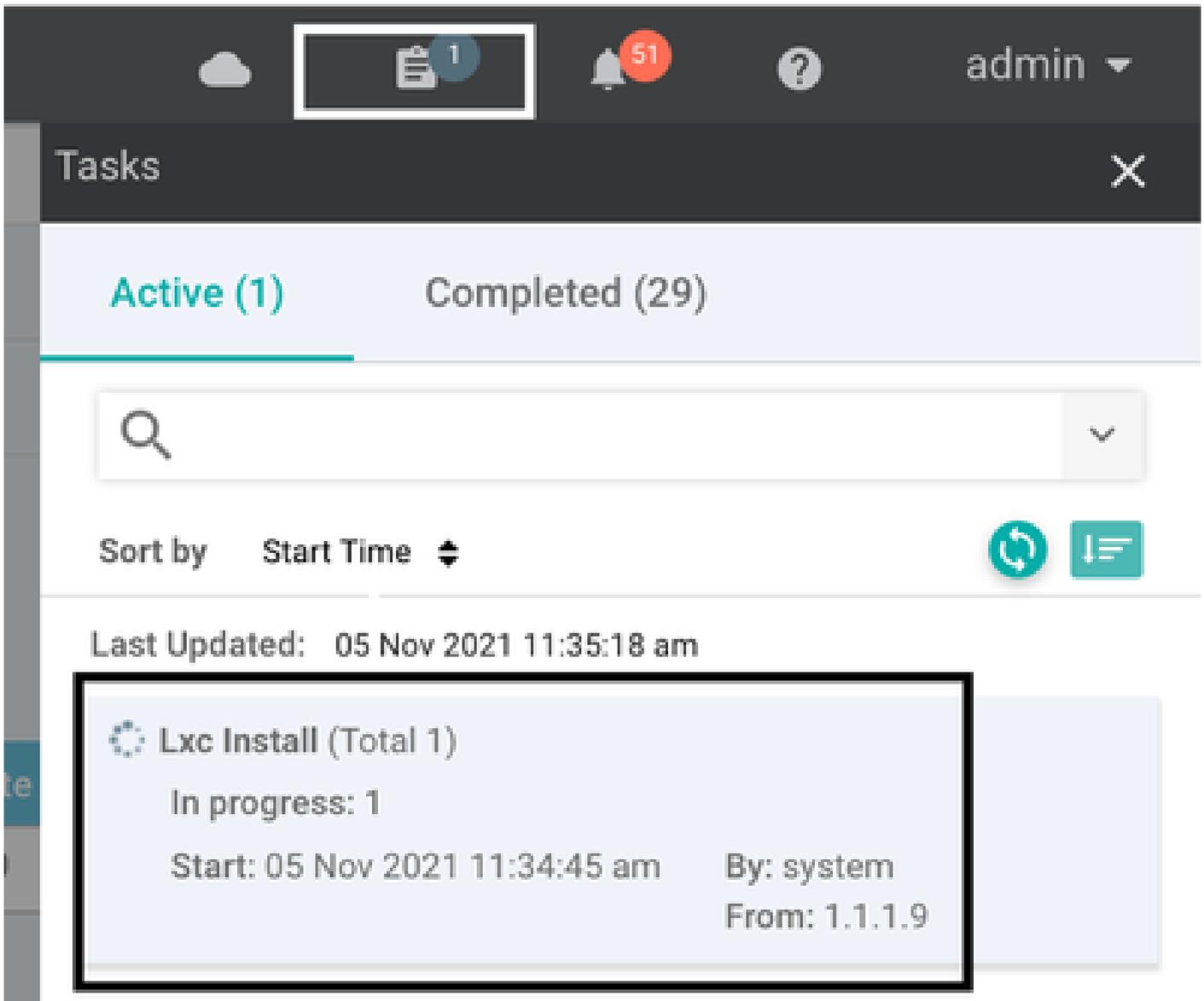
Push Feature Template Configuration | ✔ Validation Success

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

Una volta che il modello è stato spostato allo stato di programmazione, nel menu delle operazioni viene visualizzata una nuova operazione in corso. La nuova attività è l'installazione Lxc, ovvero il gestore avvia automaticamente l'installazione dell'immagine virtuale sul Cisco Edge prima di eseguire il push della nuova configurazione.



Una volta installato il contenitore LX, vManage esegue il push della configurazione pre-pianificazione con le funzionalità UTD. Non è disponibile una nuova attività per questa operazione perché la configurazione è stata pianificata in precedenza.



## Verifica

Verificare che Cisco Edge sia sincronizzato con vManage e il modello associato.







## NUMERO 1. Errore: i seguenti dispositivi non dispongono di servizi software contenitore

Attivare l'immagine virtuale.

Selezionare manutenzione > software > attiva

The screenshot displays a network management interface for 'MAINTENANCE | SOFTWARE UPGRADE'. The interface includes a navigation bar with 'WAN Edge', 'Controller', and 'vManage'. A toolbar at the top contains buttons for 'Upgrade', 'Upgrade Virtual Image', 'Activate Virtual Image', 'Delete Virtual Image', 'Activate', 'Delete Available Software', and 'Set Default Version'. Below the toolbar, there is a search bar with '70.70.70.1' and a 'Search Options' dropdown. A table lists device information:

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

An error dialog box titled 'Activate Virtual Image' is overlaid on the interface. The dialog contains the following text:

Following devices do not have container software services.  
Click 'Skip Devices' to continue activate image.

- (SAASRouter01)

The dialog has two buttons: 'Skip Devices' and 'Cancel'.

L'immagine virtuale invia un messaggio di errore: i dispositivi non dispongono di servizi software contenitore, se il router Cisco Edge selezionato non dispone di un criterio di sicurezza con il sottomodulo del profilo del contenitore.

## 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



Questo modello viene aggiunto automaticamente se si utilizza un criterio di sicurezza che include funzionalità di sicurezza quali IPS (Intrusion Prevention System), IDS (Intrusion Detection System), URL Filtering (URL-F) e AMP (Advanced Malware Protection) che richiedono un pacchetto UTD. Non tutte le funzioni di sicurezza disponibili necessitano di un motore UTD come la semplice funzione ZBFW.

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

Una volta eseguito il push del modello con il sottomodulo del profilo del contenitore, il gestore installa automaticamente l'immagine virtuale.

## NUMERO 2. Memoria disponibile insufficiente

Verificare che il router Cisco Edge disponga di 8 GB di memoria DRAM. In caso contrario, il processo di installazione Lxc che invia un dispositivo non è configurato per accettare la nuova configurazione. Errore di memoria insufficiente. Per utilizzare le funzionalità UTD, i router Cisco Edge devono avere almeno 8 GB di 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

```

In questo caso, i CSRv hanno solo 4 GB di DRAM. Dopo l'aggiornamento della memoria alla memoria DRAM da 8 GB, l'installazione è riuscita.

Verificare la memoria totale corrente con l'output show sdwan system status:

```
<#root>
```

```
Router01#
```

show sdwan system status

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

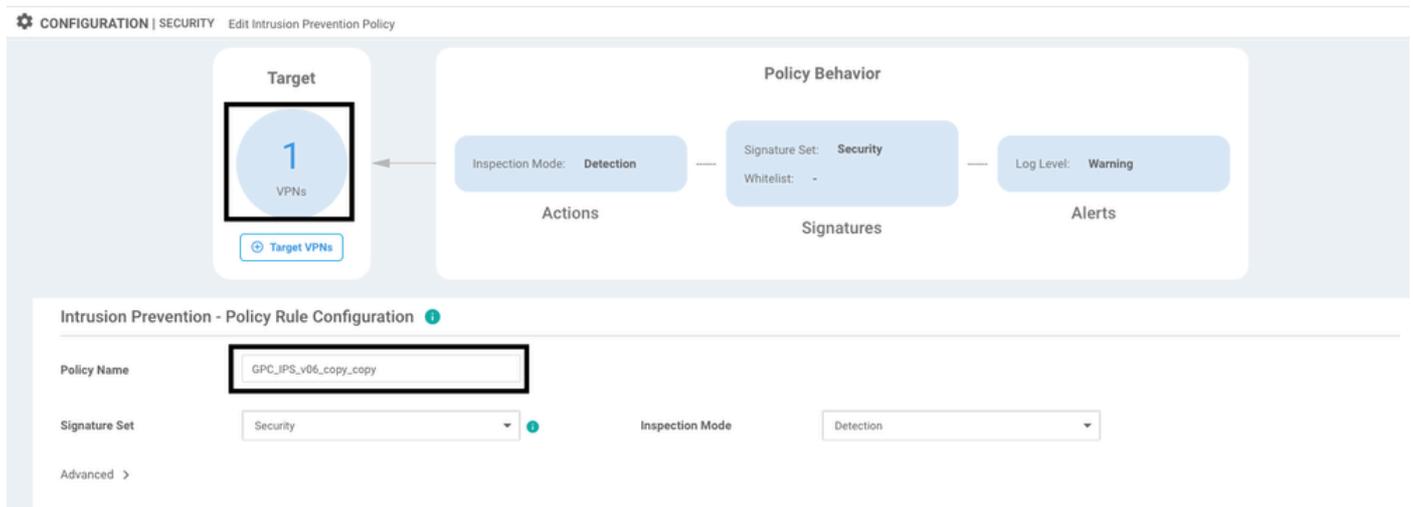
 Nota Per installare UTD deve essere disponibile una quantità di memoria sufficiente. Se la DRAM installata è adeguata ma l'installazione non riesce a causa di memoria insufficiente, controllare l'utilizzo corrente in mostra processi piattaforma di memoria ordinata

### NUMERO 3. Riferimento non valido

Verificare che le VPN/VRF utilizzate su una delle funzionalità dei criteri di sicurezza siano già configurate nel router perimetrale Cisco per evitare un riferimento non valido per le sequenze dei criteri di sicurezza.



In questo esempio, il criterio di sicurezza dispone di un criterio di prevenzione delle intrusioni per VPN/VRF 1, ma i dispositivi non dispongono di alcun VRF 1 configurato. Pertanto, il gestore invia un riferimento non valido per tale sequenza di criteri.





## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).