

# Instalar imagen virtual de seguridad UTD en routers cEdge

## Contenido

---

### [Introducción](#)

### [Prerequisites](#)

#### [Requirements](#)

#### [Componentes Utilizados](#)

#### [Antecedentes](#)

[Routers que ejecutan el software Cisco IOS XE SD-WAN \(16.x\)](#)

[Routers que ejecutan el software Cisco IOS XE \(17.x\)](#)

### [Configurar](#)

[Paso 1. Cargar imagen virtual](#)

[Paso 2. Agregar subplantilla de política de seguridad y perfil de contenedor a plantilla de dispositivo](#)

[Paso 3. Actualizar o adjuntar la plantilla de dispositivo con la política de seguridad y el perfil del contenedor](#)

### [Verificación](#)

### [Problemas comunes](#)

[PROBLEMA 1. Error: los siguientes dispositivos no tienen servicios de software de contenedor](#)

[PROBLEMA 2. Memoria disponible insuficiente](#)

[PROBLEMA 3. Referencia no válida](#)

[PROBLEMA 4. UTD está instalado y activo, pero no habilitado](#)

### [Video](#)

### [Información Relacionada](#)

---

## Introducción

Este documento describe cómo instalar la imagen virtual de seguridad de Unified Threat Defence (UTD) para habilitar las funciones de seguridad en los dispositivos SD-WAN Cisco IOS® XE.

## Prerequisites

- Antes de utilizar estas funciones, cargue la imagen virtual de seguridad correspondiente en el repositorio de vManage.
- El router Cisco Edge debe estar en modo vmanage con una plantilla previamente conectada.
- Cree una plantilla de políticas de seguridad para el sistema de prevención de intrusiones (IPS), el sistema de detección de intrusiones (IDS), el filtrado de URL (URL-F) o el filtrado de protección frente a malware avanzado (AMP).

## Requirements

- 4000 Router de servicios integrados Cisco IOS XE SD-WAN (ISR4k)
- Router de servicios integrados 1000 Cisco IOS XE SD-WAN (ISR1k)
- Router para servicios basados en la nube 1000v (CSR1kv),
- Router de servicios integrados (ISRv) 1000v
- Plataformas Cisco Edge que admiten 8 GB de DRAM.

## Componentes Utilizados

- Imagen virtual de Cisco UTD
- vManage controller
- Routers Cisco Edge con conexiones de control con controladores.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

La imagen de Cisco UTD necesita una política de seguridad en la plantilla del dispositivo que se va a instalar, así como funciones de seguridad activadas, como el sistema de prevención de intrusiones (IPS), el sistema de detección de intrusiones (IDS), el filtrado de URL (URL-F) y la protección frente a malware avanzado (AMP) en los routers periféricos de Cisco.

Descargue el software Cisco UTD Snort IP Engine del [software Cisco](#)

Utilice el regex compatible con la imagen virtual de Cisco UTD para la versión actual de Cisco IOS XE. Utilice el comando `show utd engine standard version` para validar la imagen UTD recomendada y admitida.

```
<#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 La ruta para descargar la imagen depende de si el router ejecuta Cisco IOS XE SD-WAN Software (16.x) o Cisco IOS XE Software Universal (17.x).

---

## Routers que ejecutan el software Cisco IOS XE SD-WAN (16.x)

La ruta para obtener el software Cisco UTD Snort IPS Engine es Routers/WAN definida por software (SD-WAN)/routers XE SD-WAN/y el router integrado de la serie.

The screenshot shows a navigation menu with the following structure:

- Downloads Home / Routers / Software-Defined WAN (SD-WAN)
- Left sidebar (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**
- Center column (Software-Defined WAN (SD-WAN)): 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
- Right column (Meraki vMX): Meraki vMX, SD-WAN, **XE SD-WAN Routers**, vEdge Router

Elija el tipo de modelo para el router Cisco Edge.

Nota Los routers de servicios de agregación (ASR) de la serie no están disponibles para las funciones de UTD.

The screenshot shows the navigation menu with the following structure:

- Downloads Home / Routers / Software-Defined WAN (SD-WAN) / XE SD-WAN Routers
- Left sidebar (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**
- Center column (XE SD-WAN Routers): Meraki vMX, SD-WAN, **XE SD-WAN Routers**, vEdge Router
- Right column (ASR 1000 Series IOS XE SD-WAN): ASR 1000 Series IOS XE SD-WAN, **CSR 1000V Series IOS XE SD-WAN**, ISR 1000 Series IOS XE SD-WAN, ISR 4000 Series IOS XE SD-WAN

Después de elegir el tipo de modelo de router, seleccione la opción de software Cisco IOS XE SD-WAN para obtener el paquete UTD para Cisco Edges en la versión 16.x.

The screenshot shows the software selection page with the following structure:

- 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

Nota La ruta de descarga para elegir la imagen virtual de Cisco UTD para el código 16.x

 para los routers Cisco Edge también muestra la opción de software Cisco IOS XE. Esta es la ruta para elegir los códigos de actualización de Cisco Edge solo para 17.x, pero no se encuentra la imagen virtual UTD para la versión 17.x. Cisco Unified regular Cisco IOS XE y Cisco IOS XE SD-WAN codifica en 17.x y versiones más recientes, por lo que la ruta para obtener la imagen virtual de Cisco UTD para 17.x es la misma que la de los códigos normales de Cisco IOS XE.

Elija la versión actual de Cisco Edge y descargue el paquete UTD para esa versión.

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)

[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](#)

[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	<a href="#">Download</a> <a href="#">Cart</a> <a href="#">Bookmark</a>
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	<a href="#">Download</a> <a href="#">Cart</a> <a href="#">Bookmark</a>
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	<a href="#">Download</a> <a href="#">Cart</a> <a href="#">Bookmark</a>
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	<a href="#">Download</a> <a href="#">Cart</a> <a href="#">Bookmark</a>
UTD Engine for IOS XE SD-WAN 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	<a href="#">Download</a> <a href="#">Cart</a> <a href="#">Bookmark</a>

Routers que ejecutan el software Cisco IOS XE (17.x)

Cisco IOS XE Release 17.2.1r y la versión más reciente utilizan la imagen universalk9 para implementar tanto Cisco IOS XE SD-WAN como Cisco IOS XE en los dispositivos Cisco IOS XE. El software UTD Snort IPS Engine se encuentra en 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

Después de elegir el tipo de modelo del router, seleccione el 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](#)

Seleccione la versión actual del router y descargue el paquete UTD para la versión seleccionada.

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

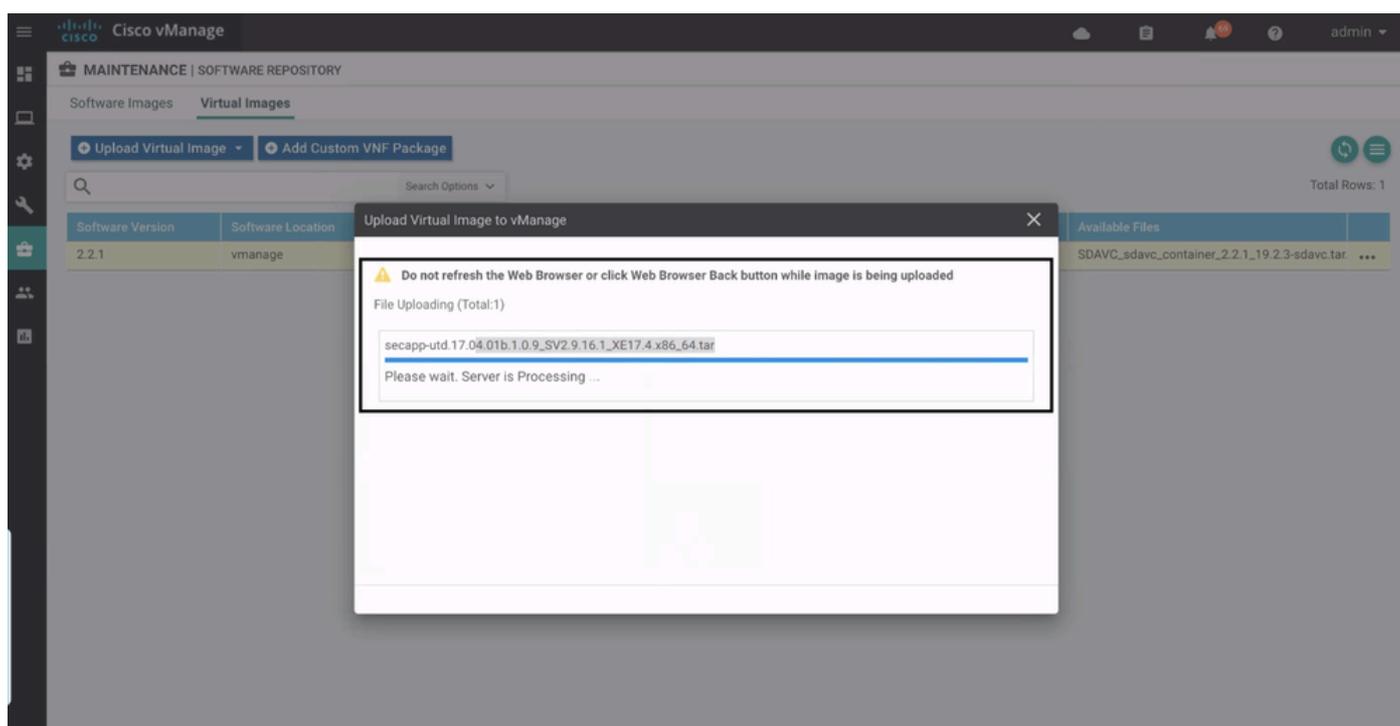
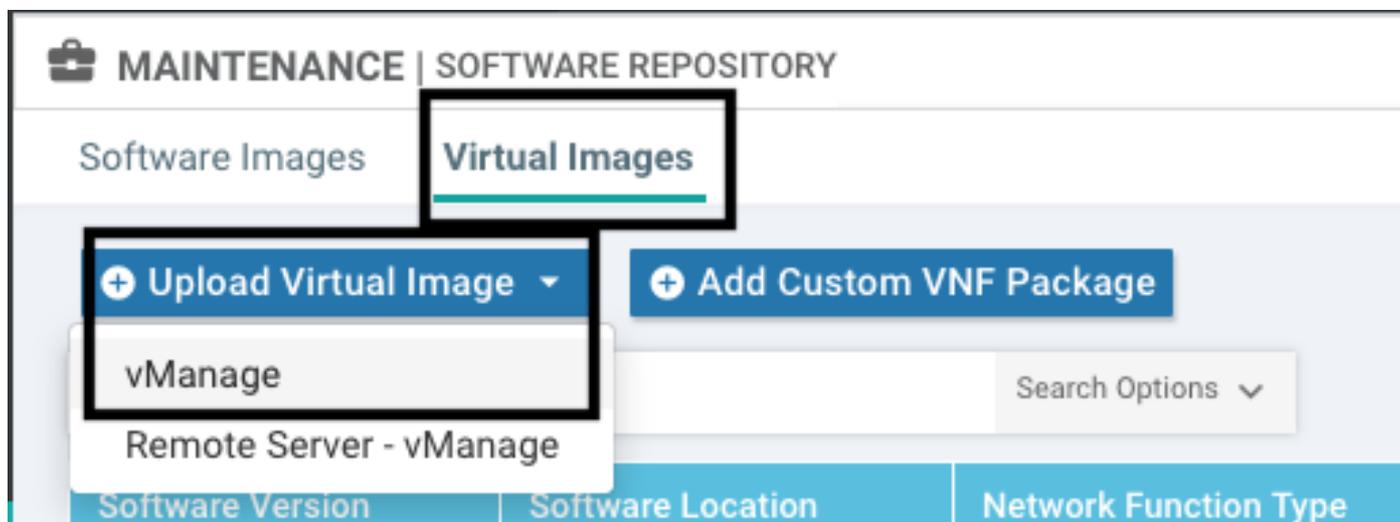
 Nota: los routers de la serie Cisco ISR1100X (routers Cisco Nutella SR1100X-4G/6G) que ejecutan el software Cisco IOS XE en lugar de Viptela Code se basan en x86\_x64. La imagen virtual de Cisco UTD publicada para ISR4K puede funcionar con ellos. Puede instalar la misma versión de código de imagen UTD de Cisco compatible con regex para la versión actual SD-WAN de Cisco IOS XE en el router Nutella. Utilice el comando `show utd engine standard version` para validar la imagen regex UTD de Cisco recomendada y admitida.

## Configurar

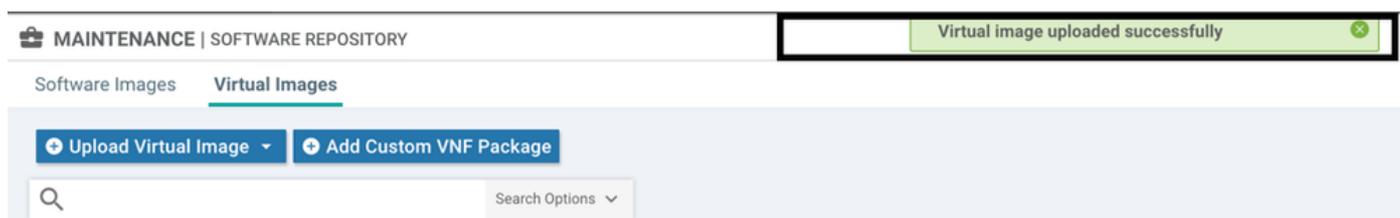
## Paso 1. Cargar imagen virtual

Asegúrese de que la imagen virtual coincida con el código SD-WAN actual de Cisco IOS XE en Cisco Edge y cárguela en el repositorio de vmanage.

Vaya a Mantenimiento > Repositorio de software > Imagen virtual > Cargar imagen virtual > vManage.



Una vez que la imagen virtual de Cisco UTD se haya cargado correctamente, vuelva a comprobar que está en el repositorio.



Cisco vManage MAINTENANCE | SOFTWARE REPOSITORY

Software Images Virtual Images

Upload Virtual Image Add Custom VNF Package

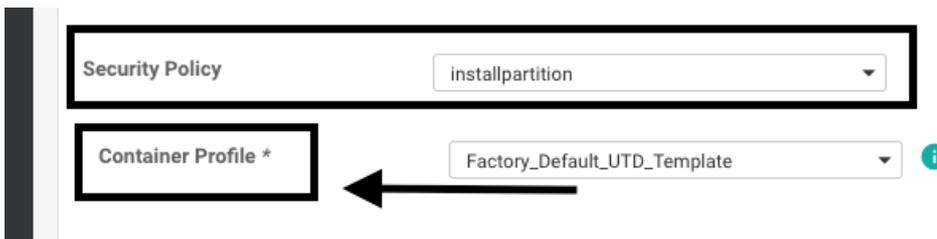
Search Options

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	aaarch64	aaarch64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-aaarch64_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	aaarch64	aaarch64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-aaarch64_1.0.10...	06 Feb 2020 9:39:51 AM ...

## Paso 2. Agregar subplantilla de política de seguridad y perfil de contenedor a plantilla de dispositivo

Agregue la política de seguridad creada anteriormente a la plantilla de dispositivo. La política de seguridad debe tener una política IPS/IDS, URL-F o de filtrado de AMP en la plantilla de dispositivo. Abra el perfil del contenedor automáticamente. Utilice el perfil de contenedor predeterminado o modifíquelo si es necesario.



## Paso 3. Actualizar o adjuntar la plantilla de dispositivo con la política de seguridad y el perfil del contenedor

Actualice o adjunte la plantilla al router Cisco Edge. Observe en config diff que se ha configurado la configuración de alojamiento de aplicaciones y el motor UTD para la función IPS/IDS, URL-F o AMP Filtering.

```
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 !
```

El estado de la plantilla cambia a Finalizado-programado debido a que vmanage observó que la configuración aplicada tiene funciones de motor UTD, por lo que vmanage determina que Cisco Edge necesita la imagen virtual instalada para usar las funciones de seguridad UTD.

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

Después de mover la plantilla al estado de programación, aparece una nueva tarea en curso en el menú de tareas. La nueva tarea es la instalación Lxc, lo que significa que vmanage inicia automáticamente la instalación de la imagen virtual en Cisco Edge antes de enviar la nueva configuración.

The screenshot shows the vManage interface. At the top, there is a navigation bar with a cloud icon, a task icon with a '1' notification, a bell icon with '51' notifications, a help icon, and the user name 'admin'. Below this is a 'Tasks' header with a close button. The main area is divided into 'Active (1)' and 'Completed (29)'. A search bar is present, followed by sorting options: 'Sort by Start Time'. There are refresh and list view icons. A summary card for 'Lxc Install (Total 1)' is highlighted with a red box, showing 'In progress: 1', 'Start: 05 Nov 2021 11:34:45 am', 'By: system', and 'From: 1.1.1.9'. The last updated time is '05 Nov 2021 11:35:18 am'.

Una vez instalado el contenedor LX, vManage realiza la configuración previa a la programación con las funciones UTD. No hay ninguna tarea nueva para esto debido a que la configuración se programó anteriormente.

The screenshot shows the 'TASK VIEW' for 'Lxc Install | Validation Success'. It indicates 'Total Task: 1 | Success: 1' and 'Initiated By: system From: 1.1.1.9'. A table with one row shows the task details:

Status	Device IP	Message	Start Time
Success	70.70.70.1	Done - Lxc Install	05 Nov 2021 12:06:03 PM CST

Below the table, a log shows the following messages:

```

[5-Nov-2021 18:06:03 UTC] Total number of Container apps to be installed: 1. Container apps to be installed are following: lapp-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE17.3]
[5-Nov-2021 18:06:03 UTC] Started 1/1 lxc container (app-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE17.3) installation
[5-Nov-2021 18:06:03 UTC] Checking if lxc is enabled on device
[5-Nov-2021 18:06:04 UTC]
[5-Nov-2021 18:06:09 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-Nov-2021 18:06:20 UTC] Connection Instance: 4, Color: biz-internet
[5-Nov-2021 18:06:20 UTC] Downloading http://1.1.1.9:8888/software/package/lxc/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?deviceId=70.70.70.1
  
```

## Verificación

Verifique si Cisco Edge está sincronizado con vManage y la plantilla adjunta.







## PROBLEMA 1. Error: los siguientes dispositivos no tienen servicios de software de contenedor

Activa la imagen virtual.

Vaya a mantenimiento > software > activar

The screenshot shows the vManage 'MAINTENANCE | SOFTWARE UPGRADE' interface. At the top, there are navigation tabs for 'WAN Edge', 'Controller', and 'vManage'. Below these are several action buttons: '1 Rows Selected', 'Upgrade', 'Upgrade Virtual Image', 'Activate Virtual Image', 'Delete Virtual Image', 'Activate', 'Delete Available Software', and 'Set Default Version'. A search bar shows '70.70.70.1' and 'Search Options'. A table below lists device details:

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 displayed in the foreground. It contains the following text:

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

- (SAASRouter01)

Buttons for 'Skip Devices' and 'Cancel' are at the bottom of the dialog.

La imagen virtual envía un error: Los dispositivos no tienen servicios de software de contenedor, si el router Cisco Edge seleccionado no tiene una política de seguridad con la subplantilla de perfil de contenedor.

## Additional Templates

AppQoS

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



Esta plantilla se agrega automáticamente si utiliza una directiva de seguridad que incluya funciones de seguridad como el sistema de prevención de intrusiones (IPS), el sistema de detección de intrusiones (IDS), el filtrado de URL (URL-F) y la protección frente a malware avanzado (AMP) que necesite el paquete UTD. No todas las funciones de seguridad disponibles necesitan un motor UTD como una simple función 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 vez que se inserta la plantilla con la subplantilla de perfil de contenedor, vmanage instala automáticamente la imagen virtual.

## PROBLEMA 2. Memoria disponible insuficiente

Asegúrese de que el router Cisco Edge tenga una memoria DRAM de 8 GB; de lo contrario, el proceso de instalación Lxc send a Device no está configurado para aceptar la nueva configuración. Error de memoria insuficiente disponible. Los requisitos para que los routers Cisco Edge utilicen las funciones UTD es tener un mínimo de 8 GB de 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, reserved memory:1048576 KB, available memory:1048576 KB

```

En este caso, el CSRv solo tiene 4 GB de DRAM. Después de actualizar la memoria a 8GB de DRAM, la instalación es un éxito.

Verifique la memoria total actual con el resultado de show sdwan system status:

```
<#root>
```

```
Router01#
```

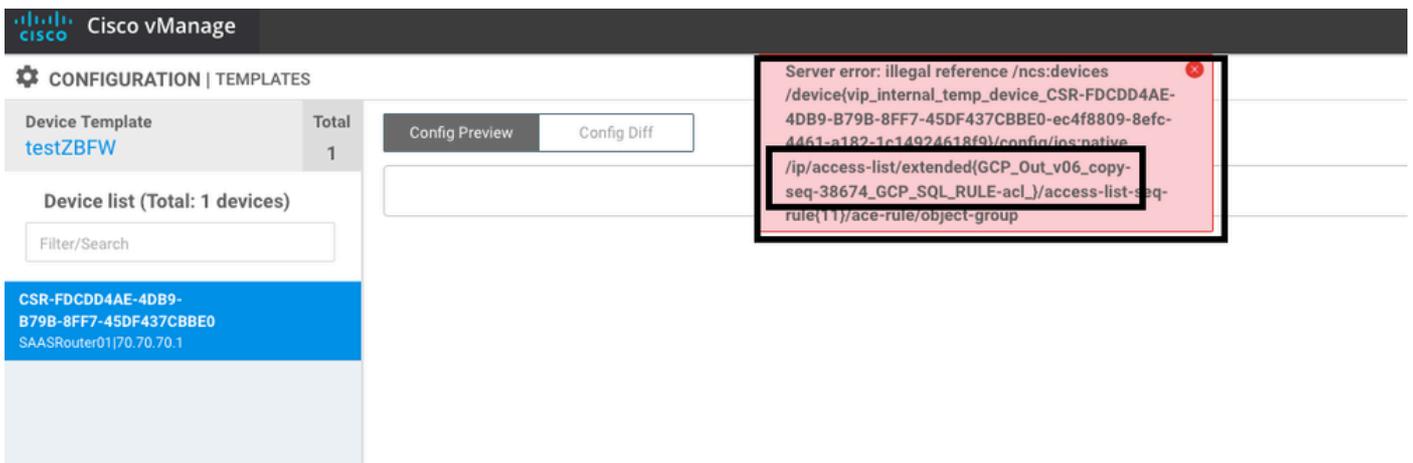
show sdwan system status

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

 Nota Debe haber suficiente memoria libre disponible para instalar UTD. Si la DRAM instalada es adecuada pero la instalación sigue fallando debido a la falta de memoria, verifique el uso actual en show processes memory platform ordenado

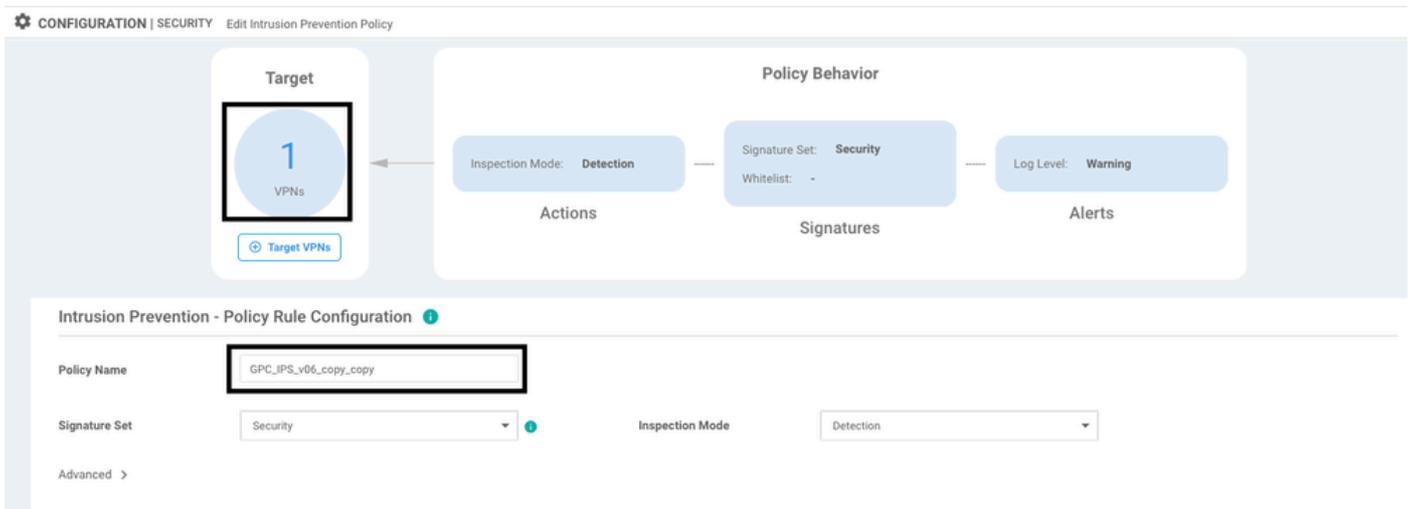
### PROBLEMA 3. Referencia no válida

Asegúrese de que las VPNs/VRFs utilizadas en cualquiera de las funciones de la política de seguridad ya estén configuradas en el router de borde de Cisco para evitar una referencia ilegal para las secuencias de la política de seguridad.



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. A device entry is visible: 'CSR-FDCDD4AE-4DB9-B79B-8FF7-45DF437CBBE0 SAASRouter01|70.70.70.1'. On the right, there is a 'Config Preview' and 'Config Diff' section. 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/ip/native /ip/access-list/extended(GCP\_Out\_v06\_copy-seq-38674\_GCP\_SQL\_RULE-acl\_/access-list-seq-rule(1))/ace-rule/object-group'. The error message is highlighted with a black border.

En este ejemplo, la política de seguridad tiene una política de prevención de intrusiones para VPN/VRF 1, pero los dispositivos no tienen ningún VRF 1 configurado. Por lo tanto, vmanage envía una referencia ilegal para esa secuencia de políticas.



The screenshot shows the Cisco vManage interface for 'CONFIGURATION | SECURITY Edit Intrusion Prevention Policy'. The 'Target' section shows a box with the number '1' and 'VPNs' below it, with a 'Target VPNs' button. The 'Policy Behavior' section shows 'Inspection Mode: Detection', 'Signature Set: Security', and 'Log Level: Warning'. Below this, there are sections for 'Actions', 'Signatures', and 'Alerts'. At the bottom, the 'Intrusion Prevention - Policy Rule Configuration' section shows 'Policy Name' as 'GPC\_IPS\_v06\_copy\_copy', 'Signature Set' as 'Security', and 'Inspection Mode' as 'Detection'. The 'Policy Name' field is highlighted with a black border.



## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).