

La implementación virtual de Secure Firewall falla debido al Extractor de archivos de Windows

Contenido

Problema

La implementación del dispositivo Cisco Secure Firewall Virtual (ASAv, FTDv, FMCv o FMCv300) en VMware vCenter o ESXi produce un error, que se muestra durante la implementación de VM:

vCenter									
Recent Tasks									
Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time		
Import OVF package	ITOps	Failed to deploy OVF package. Cause: A general system error occurred: Transfer failed: Invalid response code: 500.		vsphere.local/diungu	99 ms	04/23/2026, 12:29:31 PM	04/23/2026, 12:47:53 PM		
Deploy OVF template	ITOps	Failed to deploy OVF package. Cause: A general system error occurred: Transfer failed: Invalid response code: 500.	Copying Virtual Machine configuration	VSPHERE.LOCAL\content-library-user-3cc31137-fd28-4bd1-bf2b-ccc9babeb6d1	4 ms	04/23/2026, 12:30:50 PM	04/23/2026, 12:47:53 PM		
Clone virtual machine	RegalSQL22	Completed	Reconfiguring Virtual Mac	VSPHERE.LOCAL\horizonAd	507 ms	04/23/2026, 12:42:4	04/23/2026, 12:42:5		

La suma de comprobación MD5 del paquete se verifica en el sitio software.cisco.com. Después de descargar el archivo desde el sitio, el MD5 permanece igual y todavía no hay ninguna evidencia de ningún archivo dañado.

Advisories

Details

Description : FMCv: VMware install package for ESXi 6.5, 6.7, 7.0, 8.0

Release : 7.6.5

Release Date : 17-Feb-2026

FileName : Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-7.6.5-106.tar.gz

Size : 2142.02 MB (2246074566 bytes)

MD5 Checksum : d3a4976b8c0702b91af00623413e1bcb

SHA512 Checksum : 06343c9ad99ab33ae90854b6c1d5cde5

Documentation Landing Page Release Notes for 7.6.5 Advisories

17-Feb-2026

2340.50 MB

17-Feb-2026

2143.59 MB

17-Feb-2026

2284.81 MB

FMCv: VMware install package for ESXi 6.5, 6.7, 7.0, 8.0

Cisco_Secure_FW_Mgmt_Center_Virtual_VM

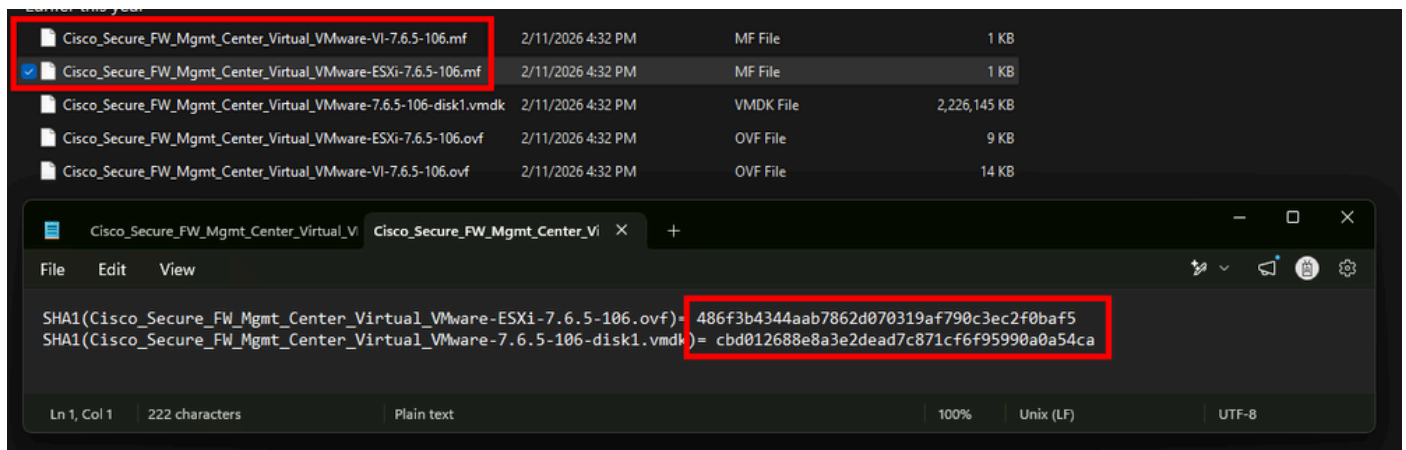
FMCv: VMware install package for ESXi 6.5, 6.7, 7.0, 8.0

6

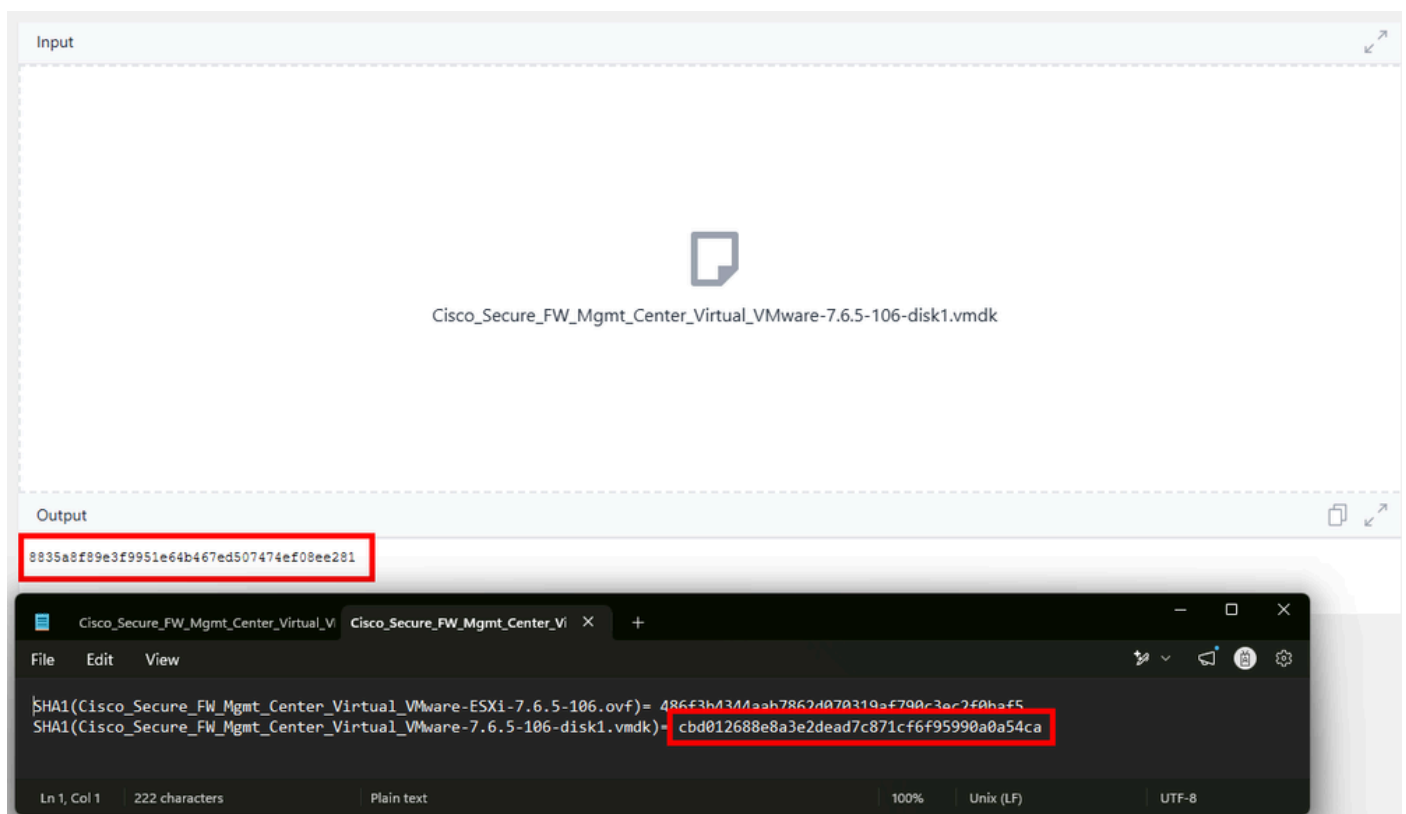
2142.02 MB

Cuando se extrae el paquete, el contenido contiene un archivo *.mf como

"Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-7.6.5-106.mf". Este archivo contiene los hashes SHA1 proporcionados por Cisco para los archivos de imagen.



Cuando se utiliza el comando nativo de Windows "Extraer todo..." en lugar de un extractor de archivos de terceros, las imágenes de se dañan y los hashes SHA1 de esos archivos no coinciden con los hashes de archivo *.mf de Cisco.



Dado que los hashes SHA1 no coinciden, los archivos dejan de ser válidos para su uso en VMWare y se produce el error 500.

! Failed to deploy OVF package.
Cause: A general system error occurred:

Transfer failed: Invalid response code: 500.

Entorno

- VMware vCenter Server 9.0 y VMware ESXi 8.0.3
- Paquetes de instalación de dispositivos virtuales de Cisco Secure Firewall mediante archivos VMDK
- Sistema operativo Windows utilizado para la extracción de paquetes y la carga en vCenter o ESXi

Resolución

Solución alternativa:

- 1.- Confirme los hashes MD5 coincidentes antes y después de la descarga del paquete VMWare comprimido.
- 2.- Descargar e instalar un extractor de archivos de terceros como 7-Zip desde un sitio web oficial para utilizar en lugar de la herramienta de extracción nativa de Windows.
- 3.- Extraiga el paquete comprimido usando el extractor de archivos de terceros y observe los hashes SHA1 para cada archivo de los archivos *.mf de Cisco en un bloc de notas.
- 4.- Generar el hash SHA1 para el archivo de imagen requerido (OVF/VMDK) con cualquier herramienta de hash en línea y asegurarse de que coincida con el que se muestra en los archivos *.mf de Cisco.
- 5.- Implemente el FMCv utilizando el archivo OVF adecuado según su método de implementación:
 - Para implementaciones de vCenter: Utilice el archivo VI OVF y VMDK

- Para implementaciones de ESXi independientes: Utilice el archivo ESXi OVF y VMDK

Causa

El problema se debe a la corrupción del archivo durante la extracción cuando se utiliza el extractor de archivos nativo de Windows para desempaquetar el paquete de instalación .tar.gz. Aunque la suma de comprobación MD5 del paquete descargado es válida, la utilidad de extracción nativa de Windows altera la integridad del archivo durante la extracción, lo que da como resultado archivos OVF/VMDK no válidos que hacen que VMware devuelva un error genérico HTTP 500 durante la implementación. Este comportamiento se alinea con el ID de bug de Cisco CSCwp3802, que documenta los problemas de extracción de imágenes virtuales de Secure Firewall mediante las herramientas nativas de Windows. Esto se resuelve con imágenes de Firepower 10.0.0.

Contenido relacionado

- [Id. de error de Cisco CSCwp33802 - \[DOC\] Error al implementar VM: error de postNFCData: \[STREAMVMDK\] CmpSize no válido leído: 3225899676](#)
- [Guía de inicio virtual de Cisco Secure Firewall Management Center](#)
- [Soporte técnico y descargas de Cisco](#)
- [Extractor de archivos 7-zip](#)
- [Herramienta Github File Checksum](#)

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).