

Virtuele implementatie van beveiligde firewall mislukt door Windows File Extractor

Inhoud

uitgifte

De implementatie van het Cisco Secure Firewall Virtual Device (ASAv, FTDv, FMCv of FMCv300)-toestel in VMware vCenter of ESXi mislukt wanneer deze fout tijdens de implementatie van de VM wordt weergegeven:

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time
Import OVF package	JTCops	Failed to deploy OVF package. Cause: A general system error occurred: Transfer failed: Invalid response code: 500.		vsphere.local/dlungu	99 ms	04/23/2026, 12:29:31 PM	04/23/2026, 12:47:53 PM
Deploy OVF template	JTCops	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-ccc9babe6d	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

De MD5 checksum van het pakket wordt geverifieerd op de site software.cisco.com. Na het downloaden van het bestand van de site, de MD5 blijft hetzelfde en er is nog geen bewijs van een beschadigd bestand.

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

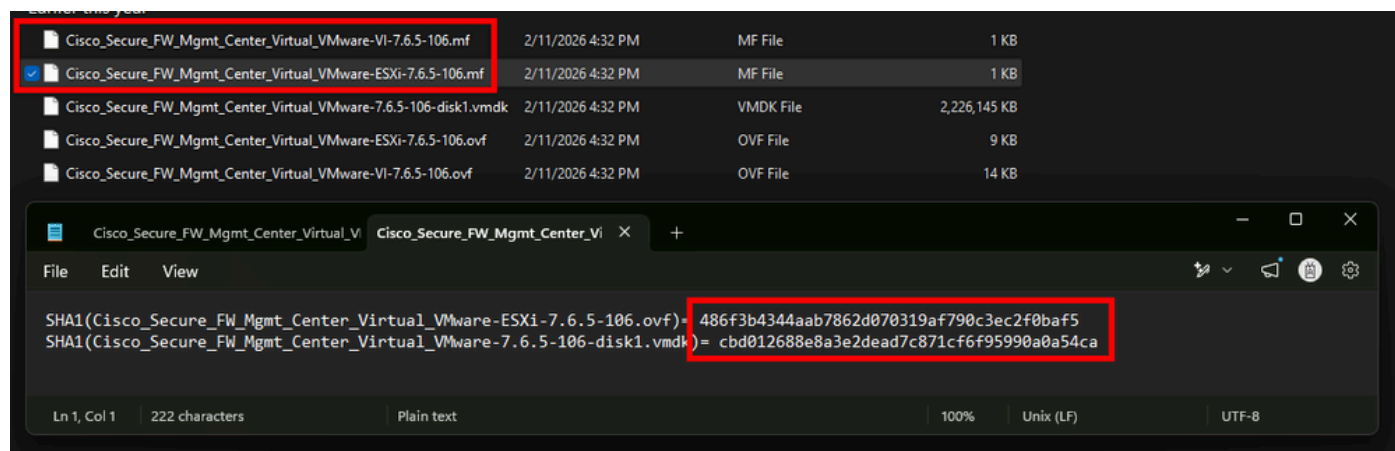
FMCv: VMware install package for ESXi 6.5, 6.7, 7.0, 8.0

Cisco_Secure_FW_Mgmt_Center_Virtual_VM

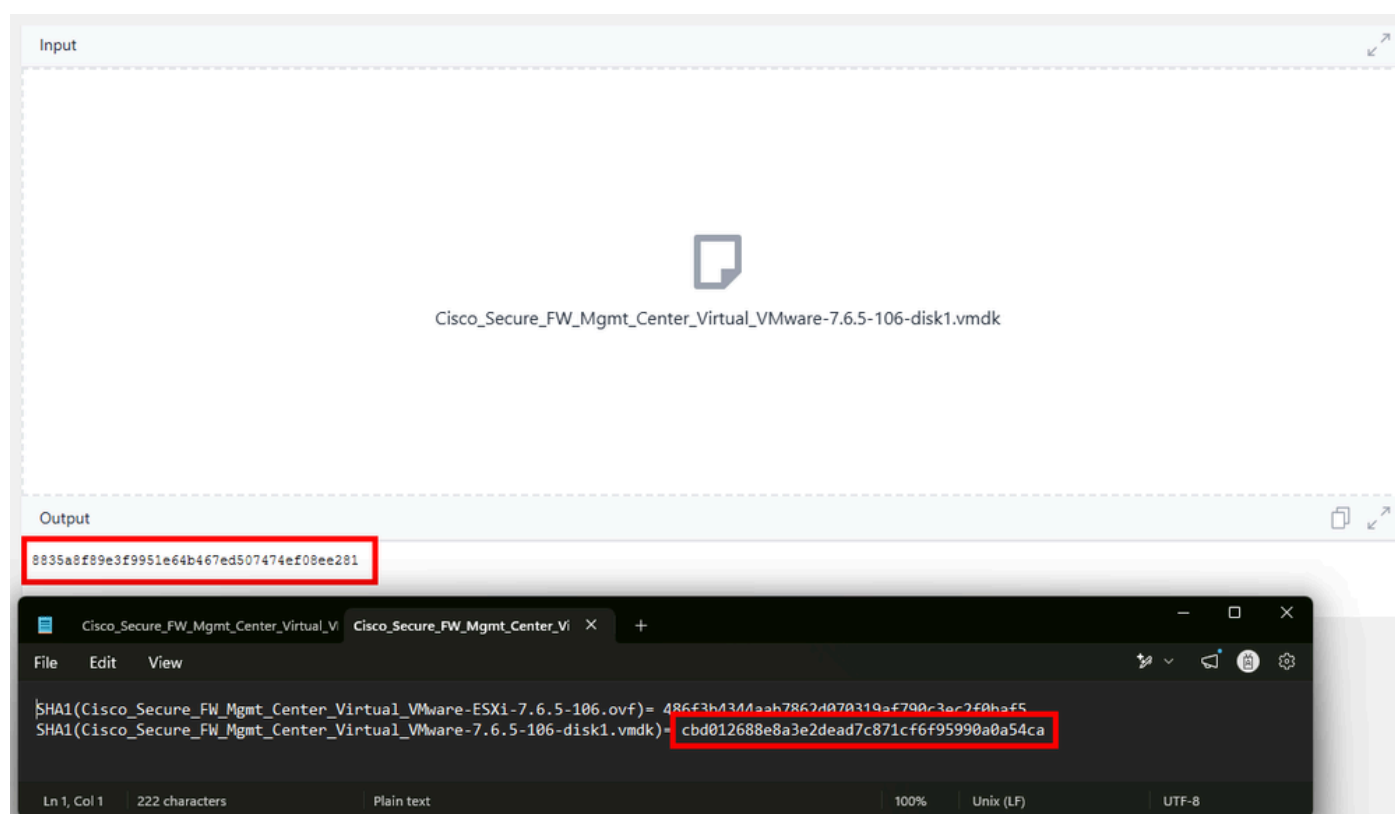
FMCv: VMware install package for ESXi 6.5, 6.7, 7.0, 8.0

2142.02 MB

Wanneer het pakket wordt geëxtraheerd, bevat de inhoud een *.mf-bestand, zoals "Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-7.6.5-106.mf". Dit bestand bevat de door Cisco verstrekte SHA1-hashes voor de afbeeldingsbestanden.



Bij gebruik van de Windows-native "Extract All..." -functie in plaats van een bestandsextractor van een derde partij, worden de afbeeldingen binnen beschadigd en komen de SHA1-hashes van die bestanden niet overeen met de *.mf-bestandshashes van Cisco.



Aangezien de SHA1-hashes niet overeenkomen, worden de bestanden ongeldig voor gebruik in VMWare en resulteert dit in de 500-fout.

! Failed to deploy OVF package.
Cause: A general system error occurred:
Transfer failed: Invalid response code: 500.

milieu

- VMware vCenter Server 9.0, VMware ESXi 8.0.3
- Cisco Secure Firewall Virtual Device Installatiepakketten met VMDK-bestanden
- Windows-besturingssysteem dat wordt gebruikt voor pakketextractie en upload naar vCenter of ESXi

resolutie

Tijdelijke oplossing:

- 1.- Bevestig de overeenkomende MD5-hashes voor en na het downloaden van het gezippte VMWare-pakket.
- 2.- Download en installeer een 3rd-party file extractor zoals 7-Zip van een officiële website te gebruiken in plaats van de Windows native extraction tool.
- 3.- Pak het pakket met rits uit met behulp van de bestandsextractor van de derde partij en noteer de SHA1-hashes voor elk bestand uit de Cisco *.mf-bestanden in een notitieblok.
- 4.- Genereer de SHA1-hash voor het vereiste beeldbestand (OVF/VMDK) met een online hashtool en zorg ervoor dat deze overeenkomt met de hash die wordt weergegeven in de Cisco *.mf-bestanden.
- 5.- Implementeer de FMCv met behulp van het juiste OVF-bestand op basis van uw implementatiemethode:
 - Voor vCenter-implementaties: gebruik het VI OVF- en VMDK-bestand

- Voor standalone ESXi-implementaties: gebruik het ESXi OVF- en VMDK-bestand

Oorzaak

Het probleem wordt veroorzaakt door bestandsbeschadiging tijdens het extraheren wanneer u de standaard Windows-bestandsextractor gebruikt om het installatiepakket .tar.gz uit te pakken. Hoewel het gedownloade MD5-controlesom van het pakket geldig is, verandert het hulpprogramma Windows Native Extraction de bestandsintegriteit tijdens het extraheren, wat resulteert in ongeldige OVF/VMDK-bestanden waardoor VMware tijdens de implementatie een algemene HTTP 500-fout teruggeeft. Dit gedrag komt overeen met Cisco bug ID CSCwp33802, die problemen documenteert bij het extraheren van virtuele afbeeldingen met behulp van Windows-native tools. Dit wordt opgelost met Firepower 10.0.0-afbeeldingen.

Gerelateerde inhoud

- [Cisco bug ID CSCwp33802 - \[DOC\] De implementatie van VM: postNFCDData is mislukt: \[STREAMVMDK\] Ongeldige cmpSize read: 3225899676](#)
- [Cisco Secure Firewall Management Center Virtual Getting Started Guide](#)
- [Cisco Technical Support en downloads](#)
- [7-zip File Extractor](#)
- [GitHub-bestand checksum, gereedschap](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.