

Virtuelle Bereitstellung der sicheren Firewall aufgrund von Windows File Extractor fehlgeschlagen

Inhalt

Problem

Die Bereitstellung des virtuellen Cisco Secure Firewall-Geräts (ASA, FTD, FMC oder FMCv300) in VMware vCenter oder ESXi schlägt mit dem folgenden Fehler fehl, der bei der VM-Bereitstellung angezeigt wird:

V7 DEM									
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\dlungu	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-3ccc31137-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		

Die MD5-Prüfsumme des Pakets wird auf der Website software.cisco.com überprüft. Nach dem Herunterladen der Datei von der Website, die MD5 bleibt die gleiche und es gibt noch keine Beweise für eine beschädigte Datei.

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	2142.02 MB

Wenn das Paket extrahiert wird, enthält der Inhalt eine *.mf-Datei wie "Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-7.6.5-106.mf". Diese Datei enthält die von Cisco bereitgestellten SHA1-Hashes für die Bilddateien.

Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-7.6.5-106.mf	2/11/2026 4:32 PM	MF File	1 KB
Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-7.6.5-106.mf	2/11/2026 4:32 PM	MF File	1 KB
Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-7.6.5-106-disk1.vmdk	2/11/2026 4:32 PM	VMDK File	2,226,145 KB
Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-7.6.5-106.ovf	2/11/2026 4:32 PM	OVF File	9 KB
Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-7.6.5-106.ovf	2/11/2026 4:32 PM	OVF File	14 KB

Cisco_Secure_FW_Mgmt_Center_Virtual_V

Cisco_Secure_FW_Mgmt_Center_Vi

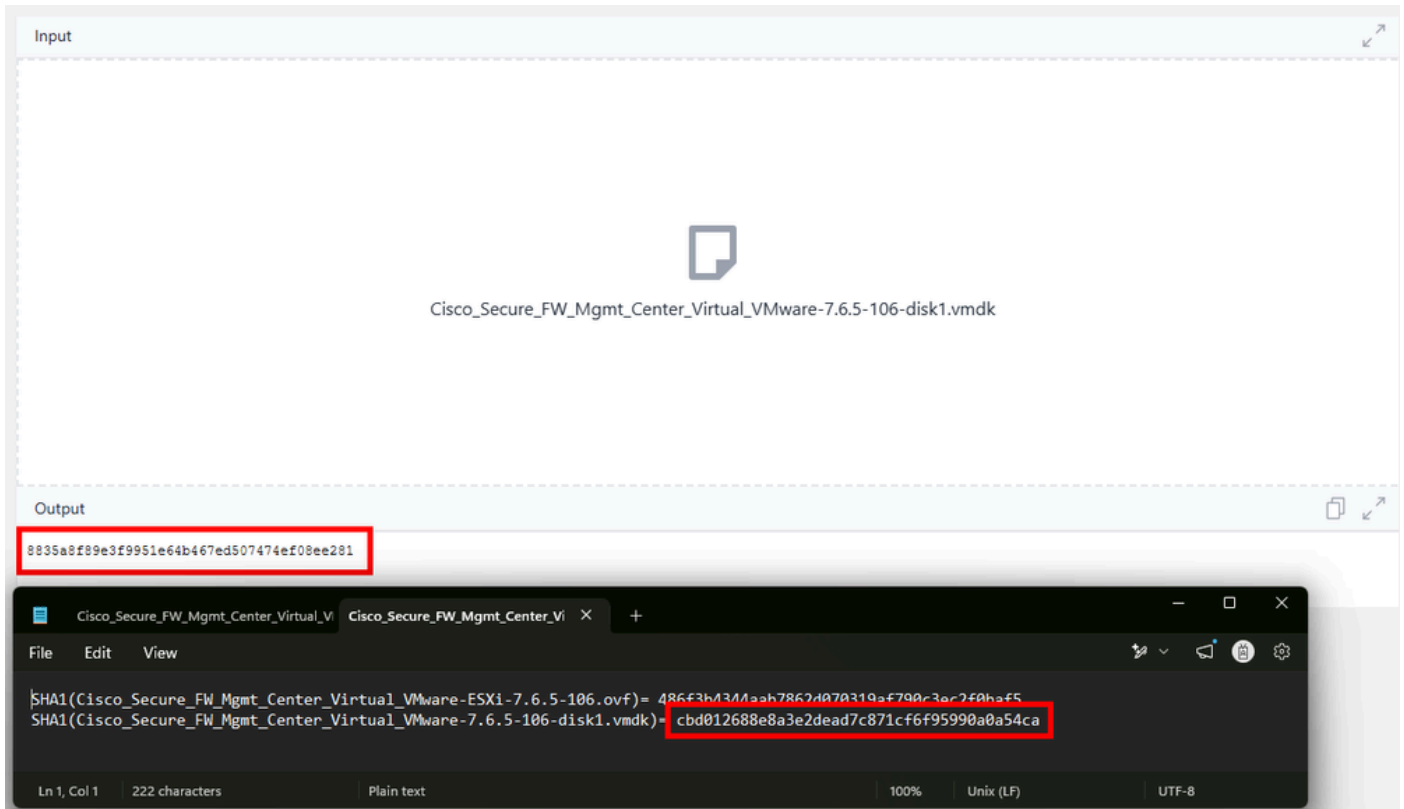
+

File Edit View

SHA1(Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-7.6.5-106.ovf)= 486f3b4344aab7862d070319af790c3ec2f0baf5
SHA1(Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-7.6.5-106-disk1.vmdk)= cbd012688e8a3e2dead7c871cf6f95990a0a54ca

Ln 1, Col 1 222 characters Plain text 100% Unix (LF) UTF-8

Bei Verwendung der nativen Windows-Option "Alle extrahieren..." -Funktion anstelle eines Dateitraktors eines Drittanbieters, die darin enthaltenen Bilder werden beschädigt, und die SHA1-Hashes dieser Dateien stimmen nicht mit den *.mf-Dateihashes von Cisco überein.



Da die SHA1-Hashes nicht übereinstimmen, werden die Dateien für die Verwendung in VMWare ungültig und führen zum 500-Fehler.

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

Umwelt

- VMware vCenter Server 9.0, VMware ESXi 8.0.3
- Installationspakete für virtuelle Cisco Secure Firewall-Geräte mit VMDK-Dateien
- Windows-Betriebssystem für Paketextraktion und Upload in vCenter oder ESXi

Auflösung

Problemumgehung:

- 1.- Bestätigen Sie übereinstimmende MD5-Hashes vor und nach dem Herunterladen des gezippten VMWare-Pakets.
- 2.- Laden Sie einen Drittanbieter-Dateiextraktor wie 7-Zip von einer offiziellen Website herunter und installieren Sie ihn anstelle des nativen Windows-Extraktionstools.
- 3.- Extrahieren Sie das gezippte Paket mit dem Dateiextraktor eines Drittanbieters, und notieren Sie die SHA1-Hashes für jede Datei aus den Cisco *.mf-Dateien in einem Notizblock.
- 4.- Generieren Sie den SHA1-Hash für die erforderliche Image-Datei (OVF/VMDK) mit einem beliebigen Online-Hash-Tool und stellen Sie sicher, dass er mit dem in den Cisco *.mf-Dateien angezeigten Hash übereinstimmt.
- 5.- Stellen Sie FMCv mit der entsprechenden OVF-Datei basierend auf Ihrer Bereitstellungsmethode bereit:
 - Für vCenter-Bereitstellungen: Verwenden der VI OVF- und VMDK-Datei
 - Für Standalone-ESXi-Bereitstellungen: Verwenden der ESXi OVF- und VMDK-Datei

Ursache

Das Problem wird durch die Dateibesädigung während der Extraktion verursacht, wenn der systemeigene Windows-Dateiextraktor zum Entpacken des .tar.gz-Installationspakets verwendet wird. Obwohl die MD5-Prüfsumme des heruntergeladenen Pakets gültig ist, ändert das native Windows-Extraktionsdienstprogramm die Dateiintegrität während der Extraktion, was zu ungültigen OVF-/VMDK-Dateien führt, die VMware während der Bereitstellung einen generischen HTTP 500-Fehler zurückgeben. Dieses Verhalten stimmt mit der Cisco Bug-ID CSCwp33802 überein, die Probleme beim Extrahieren von virtuellen Sichere Firewall-Images mithilfe nativer Windows-Tools dokumentiert. Dies wird mit Firepower 10.0.0-Images behoben.

Verwandte Inhalte

- [Cisco Bug-ID CSCwp33802 - \[DOC\] VM konnte nicht bereitgestellt werden: postNFCDData fehlgeschlagen: \[STREAMVMDK\] Ungültige cmpSize gelesen: 3225899676](#)
- [Cisco Secure Firewall Management Center - Virtueller Leitfaden für die ersten Schritte](#)
- [Technischer Support und Downloads von Cisco](#)
- [Extractor für 7-Zip-Dateien](#)
- [Github-Datei-Prüfsummentool](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.