# FMC 및 FTD에서 파일 다운로드

### 목차

## 소개

이 문서에서는 Cisco FMC(Firepower Management Center) 및 FTD(Firepower Threat Defense)에 서 로컬 컴퓨터로 로그 파일을 다운로드하는 방법을 설명합니다.

# 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Firepower 장치
- 가상 디바이스 모델

### 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

### 파일 복사

FTD에서 FMC로 파일 복사

FMC에 SCP(Secure Copy Protocol) 서버가 있으므로 파일을 FTD에서 FMC로 이동할 수 있습니다.

root@FMC:~\$ scp admin@<FTD ip>:<path to file> <path to local directory where to store>

#### 일반적인 예는 코어 파일을 FTD에서 FMC로 이동하는 것입니다.

FTD에서:

root@ciscoasa:/ngfw/var/common# ls -1
total 1557960
-rw-r--r- 1 root root 23231 Sep 6 03:43 core\_1482327396\_Firepower-module1\_snort\_6
-rw----- 1 root root 560128000 Apr 26 01:47 core\_1556242979\_ciscoasa\_snort\_6.8777
-rw------ 1 root root 383381504 Aug 25 23:05 core\_1566774281\_ciscoasa\_snort\_11.31618
-rw------ 1 root root 69562368 Aug 25 23:05 core\_1566774281\_ciscoasa\_snort\_11.31620
-rw------ 1 root root 465424384 Aug 28 02:21 core\_1566958444\_ciscoasa\_snort\_6.18352
-rw------ 1 root root 116887552 Aug 28 02:18 core\_1566958688\_ciscoasa\_snort\_6.18340
-rw------ 1 root root 52338688 Aug 28 02:18 core\_1566958689\_ciscoasa\_snort\_6.18341
-rw------ 1 root root 465514496 Sep 2 02:20 core\_1567390346\_ciscoasa\_snort\_6.27631
-rw------ 1 root root 151572480 Sep 2 02:17 core\_1567390618\_ciscoasa\_snort\_6.27435

이제 파일을 FMC로 전송합니다.

root@FMC:/Volume/home/admin# scp admin@10.10.10.10:/ngfw/var/common/core\_1567390618\_ciscoasa\_snort\_6.27

참고: 추가적인 트러블슈팅을 위해 scp 명령에서 자세한 로깅을 위해 -v를 추가합니다.

FMC에서 로컬 시스템으로 파일 복사

SCP를 사용하여 복사

FMC에 SCP(Secure Copy Protocol) 서버가 있으며 FMC에서 다른 디바이스로 이동할 수 있는 파일을 사용합니다.

root@FMC:~\$ scp <path to local directory where to store> admin@<FMC ip>:<path to file>

일반적인 방법은 코어 파일을 FMC에서 로컬 데스크톱으로 이동하는 것입니다.

root@localMachine:/Volume/home/admin# scp admin@10.10.10.20:/var/common/core\_1567390618\_ciscoasa\_snort\_

Windows에서는 자주 <u>사용되</u>는 툴인 WInSCP가 사용됩니다. 이 툴은 GUI 기반 인터페이스를 제공

#### 합니다.

In FMC 6.4 and above, SCP to the FMC is not possible directly. For that, the following is needed(the be
root@FMC:/Volume/home/admin# usermod --shell /bin/bash admin
After this SCP to the FMC will work. Once done, please remeber to rollback:

root@FMC:/Volume/home/admin# usermod --shell /usr/bin/clish admin

#### GUI에서 다운로드

존재하는 파일/var/common은 GUI에서 다운로드할 수 있습니다.

If there are any file(s) and/or tcpdump generated on the FMC, please move to /var/common, so that it ca

1단계. 그림과 같이 System > Health > Monitor로 이동하고 파일을 다운로드해야 하는 센서를 클릭 합니다.

0.01	in realizer router betters object			Configuration	110000	Demoires	Internation	Undation	Linner	Health & Mealter	Man Andrews	Tasks
				Configuration	Users	Domains	Incegration	opdates	Licenses •	rieann - Honitor	Monitoring +	TOOIS •
												Alerts
	Status	Count		Applia	ince Stati	is Summary						
×	Error	0										
0	Critical	1										
	Warning	0					Normal (50.00%)					
0	Recovered	0										
0	Normal	1										
×	Disabled	0		Gritical (50.00%)	-							
1	Appliance	Description										
-		Critical Modul	s: 1 Normal Modules: 17 Disabled	f Modules:15								
0	firepower (Part Blacklisted)	ModuleSmart	License Monitor: Smart License u	isage is out of compliance								

2단계. 그림과 같이 System > Health > Monitor로 이동하여 Advanced Troubleshooting을 클릭합니 다.

Image: Configuration       Users       Density       Teggration       Users       Users       Health + Honitor       Meeting of Tools         Appliance       Module Status Surrnary       Modue Status Surrnary       Modue Status	Jven	new Analysis Policies Devices Objects Amp	Intemgence			asheel.	S System		
Hadiance Applance reproduct (Part Blacklisted) Reproduct (Part Blacklisted) Reproduct Troubleshooting Retworked Troubleshoo				Configuration Users Domains Integ	gration Updates Licenses •	Health + Mor	nitor Monitor	ring • Tools •	
Modile Status Summary         Mary       Mary         Modile Status Summary         Mary       Mary         Modile Status Summary         Mary       Mary         Mary       Mary         Mary       Mary         Mary       Mary         Mary       Mary <th colspa<="" th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>Alerts</th></th>	<th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>Alerts</th>								Alerts
Applance       Module Status Summary         Improver (Part Blacklisted)       Generate Troubleshooting Tites         Advanced Troubleshooting       Module Status Summary         Improver (Part Blacklisted)       Generate Troubleshooting         Advanced Troubleshooting       Module Status Summary         Improver (Part Blacklisted)       Generate Troubleshooting         Module Status Summary       Module Status Summary         Module Status Summary       Status Summary         Mether Detail (fitepower)       Status Summary         Mether Detail (fitepower)       Status Summary         Mether Detail (fitepower)       Status Summary         Status Summary       Status Summary         Mether Detail (fitepower)       Status Summary	lealt	h Monitor							
<ul> <li>frepower (Part Blacklisted)</li> <li>frepower (Part Blacklist</li></ul>		Appliance		Module Status Sum	mary				
Advanced Troubleshooting       Deside (15.5%)       Deside (15.5%)         Nerrel (51.5%)       Oricid (3.0%)         Advanced Troubleshooting       Nerrel (51.5%)       Oricid (3.0%)         Alert       Immed (51.5%)       Oricid (3.0%)         Smart License Wenter       Smart License usage is out of compliance       Run       Events         Smart License Monitor       2019-09-02 21:47:23       All appliances are sending heart beacks correctly       Run       Events         Backlog Status       2019-09-02 21:47:23       No event backlog exists on any device       Run       Events         Backlog Status       2019-09-02 21:47:23       No event backlog exists on any device       Run       Events         Cassic License Monitor       2019-09-02 21:47:23       No event backlog exists on any device       Run       Events         Status       2019-09-02 21:47:23       No event backlog exists on any device       Run       Events       Graph         Cassic License Monitor       2019-09-02 21:47:23       No event backlog exists on any device       Run       Events       Graph         Disk Usage - Disk Heat       2019-09-02 21:47:23       No event backlog exists on any device       Run       Events       Graph         Disk Usage - Disk Heat       2019-09-02 21:47:23       No event backlog exists on any de		firepower (Part Blacklisted)	Generate Troubleshooting Files						
Alert       Time       Description       • Dissular       Run All Hoddes         Image: International Status       Smart License Monitor       2019-09-02 21:47:23       Smart License usage is out of compliance       Run       Events       Graph         Image: International Status       2019-09-02 21:47:23       All appliances are sending heartbeats correctly       Run       Events       Graph         Image: International Status       2019-09-02 21:47:23       No event backlog exists on any device       Run       Events       Graph         Image: International Status       2019-09-02 21:47:23       Licenses are up to date       Run       Events       Graph         Image: International Status       2019-09-02 21:47:23       Licenses are up to date       Run       Events       Graph         Image: International Status       2019-09-02 21:47:23       Licenses are up to date       Run       Events       Graph         Image: International Status       2019-09-02 21:47:23       Licenses are up to date       Run       Events       Graph         Image: International Status       2019-09-02 21:47:23       Licenses are up to date       Run       Run       Events       Graph         Image: International Status       2019-09-02 21:47:23       Not in HA       Run       Events       Graph       Events			Advanced Troubleshooting	James K1 5 K	Clisabled (45.45%)				
Image: Smart License Monitor       2019-09-02 21:47:23       Smart License usage is out of compliance       Run       Events       Graph         Image: Smart License Monitor       2019-09-02 21:47:23       All appliances are sending heartbeats correctly       Run       Events         Image: Bocklog Status       2019-09-02 21:47:23       No event backlog exists on any device       Run       Events         Image: Classic License Monitor       2019-09-02 21:47:23       Licenses are up to date       Run       Events       Graph         Image: Classic License Monitor       2019-09-02 21:47:23       Licenses are up to date       Run       Events       Graph         Image: Disk Usage - Disk Test       2019-09-02 21:47:23       / using 39%: 1:3G (2:2G Avail) of 3.7G       Run       Events       Graph         Image: PMC HA Status       2019-09-02 21:47:23       Not in HA       Run       Events       Graph         Image: Hardware Alarms       2019-09-02 21:47:23       Not in HA       Run       Events       Events				and the second	Gritical (3.03%)				
Image: Splance Hearbeat         Appliance Hearbeats         Appliances are sending hearbeats correctly         Run         Events           Image: Splance Hearbeat         2019-09-02 21:47:23         No event backlog exists on any device         Run         Events           Image: Splance Hearbeat         2019-09-02 21:47:23         No event backlog exists on any device         Run         Events         Graph           Image: Splance Hearbeat         2019-09-02 21:47:23         Licenses are up to date         Run         Events         Graph           Image: Splance Hearbeat         2019-09-02 21:47:23         / using 39%: 1.3G (2.G Avail) of 3.7G         No         Run         Events         Graph           Image: Splance Hearbeat         2019-09-02 21:47:23         Not in HA         Run         Events         Graph           Image: Splance Hearbeat         2019-09-02 21:47:23         Not in HA         Run         Events         Events           Image: Splance Hearbeat         2019-09-02 21:47:23         Not in HA         Run         Events         Events	Alert	Detail (firepower) Alert	Time	Description	Onical (3.03%) •.Display	Run Ali Me	odules		
Image: Seaklog Status     2019-09-02 21:47:23     No event backlog exists on any device     Run     Events       Image: Seaklog Status     2019-09-02 21:47:23     Licenses are up to date     Run     Events     Graph       Image: Seaklog Status     2019-09-02 21:47:23     Licenses are up to date     Run     Events     Graph       Image: Seaklog Status     2019-09-02 21:47:23     / using 39%: 1.3G (2.2G Avail) of 3.7G     Not     Run     Events     Graph       Image: Seaklog Status     2019-09-02 21:47:23     Not in HA     Not     Run     Events       Image: Seaklog Status     2019-09-02 21:47:23     Not in HA     Run     Events	Alert	Detail (firepower) Alert Smart License Monitor	Time 2019-09-02 21:47:23	Description Smart License usage is out of compliance	- Omor (3.03%) • Diselay	Run Ali Mo Run	odules Events	Graph	
Classic License Monitor         2019-09-02 21:47:23         Licenses are up to date         Run         Events         Graph           Disk Usage - Disk Test         2019-09-02 21:47:23         / using 39%: 1.3G (2.2G Avail) of 3.7G         •         Run         Events         Graph           PMC HA Status         2019-09-02 21:47:23         Not in HA         Run         Events         Events         Graph           Hardware Alarms         2019-09-02 21:47:23         Nation ing normally         Run         Events         Events	Alert O	Detail (firepower) Alert Smart License Monitor Appliance Heartbeat	Time 2019-09-02 21:47:23 2019-09-02 21:47:23	Description Smart License usage is out of compliance All appliances are sending heartbeats correctly	Omor (3.03%) • Disolay	Run All Mo Run Run	edules Events Events	Graph	
Image: Section Control Contro Control Contro Control Control Control Control Control Control Co	Alert O O	Detail (firepower) Alert Smart License Monitor Appliance Heartbeat Backlog Status	Time 2019-09-02 21:47:23 2019-09-02 21:47:23 2019-09-02 21:47:23	Description  Smart License usage is out of compliance  All appliances are sending heartbeats correctly No event backlog exists on any device	Once (3.03%) • Diselay	Run Ali M Run Run Run	Events Events Events	Graph	
Image: PMC HA Status         2019-09-02 21:47:23         Not in HA         Run         Events           Image: Hardware Alarms         2019-09-02 21:47:23         Hardware is functioning normally         Run         Events	Alert O O O	Detail (firepower) Alert Smart License Monitor Appliance Heartbeat Backlog Status Classic License Monitor	Time 2019-09-02 21:47:23 2019-09-02 21:47:23 2019-09-02 21:47:23 2019-09-02 21:47:23	Description Smart License usage is out of compliance All appliances are sending heartbeats correctly No event backlog exists on any device Licenses are up to date	Once (3.03%)	Run All M Run Run Run Run	events Events Events Events Events	Graph Graph	
Mardware Alarms 2019-09-02 21:47:23 Hardware is functioning normally Run Events	Alert O O O O	Detail (firepower) Alert Smart License Monitor Appliance Heartbeat Backlog Status Classic License Monitor Disk Usage - Disk Test	Time 2019-09-02 21:47:23 2019-09-02 21:47:23 2019-09-02 21:47:23 2019-09-02 21:47:23 2019-09-02 21:47:23	Description           Smart License usage is out of compliance           All appliances are sending heartbeats correctly           No event backlog exists on any device           Licenses are up to date           / using 39%: 1.3G (2.2G Avail) of 3.7G	- Once (3.03%)	Run All M Run Run Run Run Run	Events Events Events Events Events Events	Graph Graph Graph	
	Alert O O O O O	Detail (firepower) Alert Smart License Monitor Appliance Heartbeat Backlog Status Classic License Monitor Disk Usage - Disk Test FMC HA Status	Time 2019-09-02 21:47:23 2019-09-02 21:47:23 2019-09-02 21:47:23 2019-09-02 21:47:23 2019-09-02 21:47:23	Description           Smart License usage is out of compliance           All appliances are sending heartbeats correctly           No event backlog exists on any device           Licenses are up to date           / using 3%: 1.3G (2.2G Avail) of 3.7G           Not in HA	• Display	Run All Mo Run Run Run Run Run Run	edules Events Events Events Events Events Events	Graph Graph Graph	

#### 3단계. 이미지에 표시된 대로 파일 이름을 입력하고 다운로드를 클릭합니다.



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.