

# ASA 55xx-X 디바이스에서 Firepower Threat Defense 설치 및 업그레이드

## 목차

[소개](#)

[목표](#)

[사용되는 구성 요소](#)

[FTD 소프트웨어 다운로드](#)

[토폴로지](#)

[작업 1 - 사전 요구 사항 확인](#)

[작업 2 - ASA5508-X ROMMON 업그레이드](#)

[작업 3 - ASA55xx-X에 FTD 부트 이미지 설치](#)

[방법 1 - ROMMON에서](#)

[방법 2 - ASA 모드에서](#)

[작업 4 - ASA55xx-X에 FTD 시스템 이미지 설치](#)

[작업 5 - FMC에 FTD 등록](#)

[작업 6 - FTD 업그레이드](#)

[작업 7 - ASA 엔진 CLI 모드로 진입 및 CLI 모드에서 분리](#)

[작업 8 - 기존 FTD 설치 이미지로 다시 설치](#)

[단계 요약](#)

[세부 단계](#)

[관련 문서](#)

## 소개

FTD(Firepower Threat Defense)는 다음 플랫폼에 설치할 수 있는 통합 소프트웨어 이미지입니다.

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR4100, FPR9300
- VMware(ESXi)
- AWS(Amazon Web Services)
- KVM
- ISR 라우터 모듈

## 목표

이 문서의 목표는 다음 내용을 설명하는 것입니다.

- ASA5508-X 및 ASA5512-X 플랫폼에서 FTD 버전 6.0.0 설치
- FTD를 버전 6.0.0에서 6.0.1로 업그레이드하는 절차

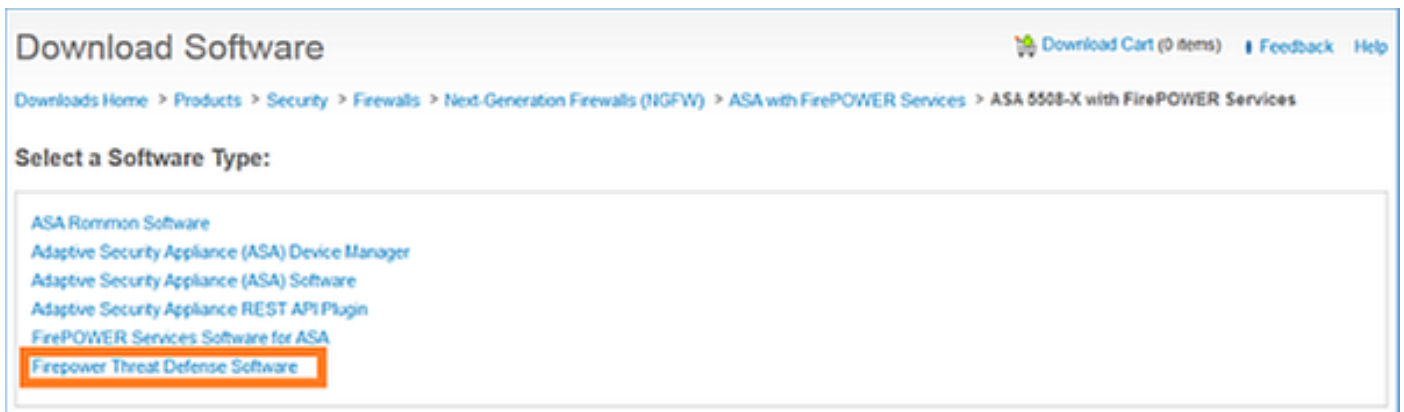
- FMC(Firepower Management Center) 등록 및 기본 라이선싱

## 사용되는 구성 요소

- ASA5508-X
- ASA5512-X
- 6.0.1(빌드 1213)을 실행하는 FMC(FireSIGHT Management Center)

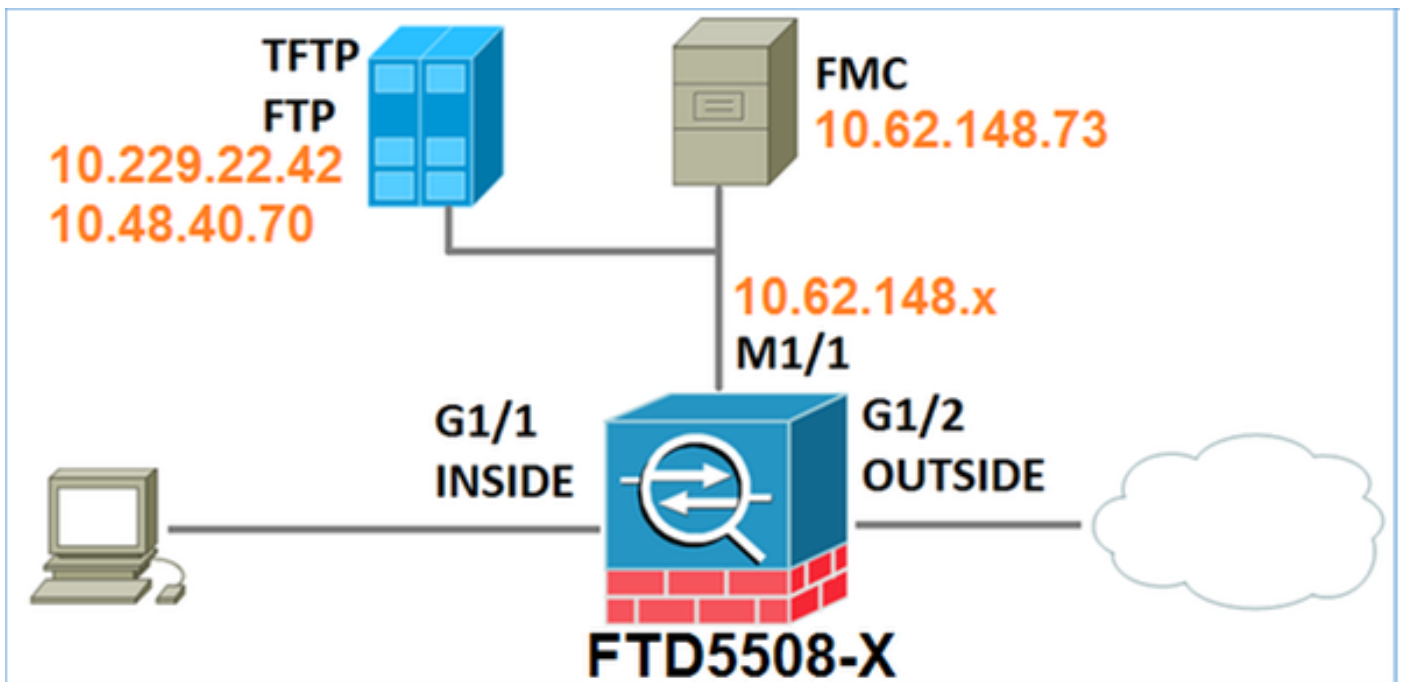
## FTD 소프트웨어 다운로드

Next-Generation Firewalls (NGFW)(NGFW(차세대 방화벽)) > ASA with FirePOWER Services > ASA 5508-X with FirePOWER Services로 이동하여 Firepower Threat Defense Software(Firepower Threat Defense 소프트웨어)를 선택합니다.



ASA5512-X 소프트웨어의 경우에도 마찬가지입니다.

## 토폴로지



## 작업 1 - 사전 요구 사항 확인

FTD 설치 전에 사전 요구 사항을 확인합니다.

### 해결책

FTD를 설치할 때는 다음의 2개 이미지를 사용합니다.

1. OS 이미지(부트 이미지) - ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, ASA5516-X에 Firepower Threat Defense를 설치하는 경우에는 \*.lfbff 파일이며, Saleen(ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X)에 Firepower Threat Defense를 설치하는 경우에는 \*.cdisk 파일입니다.
2. 시스템 이미지 - .pkg 파일입니다.

FTD 설치를 진행하기 전에 다음을 확인합니다.

- ASA 플래시에 3.1GB 이상(3GB + 부트 이미지 크기)의 여유 공간이 있어야 합니다.
- 부트 이미지는 TFTP 서버에 업로드됩니다.
- 시스템 이미지는 HTTP 또는 FTP 서버에 업로드됩니다.
- ASA5506/08/16에서는 ROMMON의 버전이 1.1.8 이상이어야 합니다.

### 여유 공간 확인:

```
FTD5508X# show flash | i free 7859437568 bytes total (4273819648 bytes free)
```

### 이미지 확인

파일 이름	설명
ftd-boot-9.6.1.0.lfbff	5506/5508/5516용 v6.0.1 Firepower Threat Defense 부트 이미지 5506/5508/5516에 새로 설치하는 데 사용할 수 있는 부트 이미지입니다.
ftd-boot-9.6.1.0.cdisk	ASA 5512/5515/5525/5545/5555용 v6.0.1 Firepower Threat Defense 부트 이미지 5512/5515/5525/5545/5555에 새로 설치하는 데 사용할 수 있는 부트 이미지입니다. 지원되는 모든
ftd-6.0.0-1005.pkg	ASA(5506/5508/5512/5515/5516/5525/5545/5555)용 v6.0.0 Firepower Threat Defense 새로 설치하는 데 사용할 수 있는 시스템 이미지입니다.

## 작업 2 - ASA5508-X ROMMON 업그레이드

사전 요구 사항에서 설명한 것처럼 ASA5506-X, ASA5508-X 및 ASA5516-X 디바이스의 ROMMON 버전은 v1.1.8이어야 합니다. 그렇지 않은 경우 Cisco ASA 다운로드 페이지에서 제공되는 asa5500-firmware-1108.SPA를 설치합니다.

### 작업 요건

ASA5508 ROMMON을 1.1.1에서 1.1.8로 업그레이드합니다.

### 해결책

업그레이드 절차는 [ASA ROMMON 업그레이드 가이드](#)에 설명되어 있습니다.

### 1단계

## 기존 ROMMON 버전을 확인합니다.

```
FTD5508X#show module Mod Card Type Model Serial No. -----  
----- 1 ASA 5508-X with FirePOWER services, 8GE, AC, ASA5508  
JAD192100SZ sfr FirePOWER Services Software Module ASA5508 JAD192100SZ Mod MAC Address Range Hw  
Version Fw Version Sw Version -----  
----- 1 188b.9d1e.ca7c to 188b.9d1e.ca84 1.0 1.1.1 9.5(2) sfr 188b.9d1e.ca7b to  
188b.9d1e.ca7b N/A N/A 5.4.1-211
```

## 2단계

## ASA의 플래시에 ROMMON 펌웨어를 다운로드합니다.

```
FTD5508X# copy ftp://10.48.40.70/ANG/mzafeiro/asa5500-firmware-1108.SPA disk0:asa5500-firmware-  
1108.SPA Address or name of remote host [10.48.40.70]? Source filename [ANG/mzafeiro/asa5500-  
firmware-1108.SPA]? Destination filename [asa5500-firmware-1108.SPA]? Accessing  
ftp://10.48.40.70/ANG/mzafeiro/asa5500-firmware-1108.SPA...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
Done! Computed Hash SHA2: d824bdeeeceel308fc64427367fa559e9 eefe8f182491652ee4c05e6e751f7a4f  
5cdea28540cf60acde3ab9b65ff55a9f 4e0cfb84b9e2317a856580576612f4af Embedded Hash SHA2:  
d824bdeeeceel308fc64427367fa559e9 eefe8f182491652ee4c05e6e751f7a4f  
5cdea28540cf60acde3ab9b65ff55a9f 4e0cfb84b9e2317a856580576612f4af Digital signature successfully  
validated Writing file disk0:/asa5500-firmware-1108.SPA... !!!!!!!!!!! 9241408 bytes copied in  
18.890 secs (513411 bytes/sec)
```

## 3단계

## ASA ROMMON 이미지를 업그레이드합니다.

```
FTD5508X# upgrade rommon disk0:asa5500-firmware-1108.SPA Verifying file integrity of  
disk0:/asa5500-firmware-1108.SPA Computed Hash SHA2: d824bdeeeceel308fc64427367fa559e9  
eefe8f182491652ee4c05e6e751f7a4f 5cdea28540cf60acde3ab9b65ff55a9f  
4e0cfb84b9e2317a856580576612f4af Embedded Hash SHA2: d824bdeeeceel308fc64427367fa559e9  
eefe8f182491652ee4c05e6e751f7a4f 5cdea28540cf60acde3ab9b65ff55a9f  
4e0cfb84b9e2317a856580576612f4af Digital signature successfully validated File Name :  
disk0:/asa5500-firmware-1108.SPA Image type : Release Signer Information Common Name : abraxas  
Organization Unit : NCS_Kenton_ASA Organization Name : CiscoSystems Certificate Serial Number :  
55831CF6 Hash Algorithm : SHA2 512 Signature Algorithm : 2048-bit RSA Key Version : A  
Verification successful. System config has been modified. Save? [Y]es/[N]o: Y  
Cryptochecksum: cb47de8a cad3b773 7fc07212 3e76ef4f
```

2804 bytes copied in 0.260 secs

Proceed with reload? [confirm]

```
*** ** START GRACEFUL SHUTDOWN --- *** ** Message to all terminals: *** ** Performing  
upgrade on rom-monitor. Shutting down License Controller Shutting down File system *** ** ---  
SHUTDOWN NOW --- *** ** Message to all terminals: *** ** Performing upgrade on rom-monitor.  
Process shutdown finished Rebooting.... INIT: Sending processes the TERM signal Deconfiguring  
network interfaces... done. Sending all processes the TERM signal... Sending all processes the  
KILL signal... Deactivating swap... Unmounting local filesystems... Rebooting... Rom image  
verified correctly Cisco Systems ROMMON, Version 1.1.01, RELEASE SOFTWARE Copyright (c) 1994-  
2014 by Cisco Systems, Inc. Compiled Mon 10/20/2014 15:59:12.05 by builder Current image  
running: Boot ROM0 Last reset cause: PowerCycleRequest DIMM Slot 0 : Present DIMM Slot 1 :  
Present INFO: Rommon upgrade state: ROMMON_UPG_START (1) INFO: Reset code: 0x00002000 Firmware  
upgrade step 1... Looking for file 'disk0:asa5500-firmware-1108.SPA' Located 'asa5500-firmware-  
1108.SPA' @ cluster 856765.  
#####  
Image base 0x77014018, size 9241408 LFBFF signature verified. Objtype: lfbff_object_rommon  
(0x800000 bytes @ 0x77014238) Objtype: lfbff_object_fpga (0xd0100 bytes @ 0x77814258) INFO: FPGA  
version in upgrade image: 0x0202 INFO: FPGA version currently active: 0x0202 INFO: The FPGA  
image is up-to-date. INFO: Rommon version currently active: 1.1.01. INFO: Rommon version in  
upgrade image: 1.1.08. Active ROMMON: Preferred 0, selected 0, booted 0 Switching SPI access to  
standby rommon 1. Please DO NOT reboot the unit, updating ROMMON..... INFO:  
Duplicating machine state..... Reloading now as step 1 of the rommon upgrade process...  
Toggling power on system board... Rom image verified correctly Cisco Systems ROMMON, Version
```

```
1.1.01, RELEASE SOFTWARE Copyright (c) 1994-2014 by Cisco Systems, Inc. Compiled Mon 10/20/2014
15:59:12.05 by builder Current image running: Boot ROM0 Last reset cause: RP-Reset DIMM Slot 0 :
Present DIMM Slot 1 : Present INFO: Rommon upgrade state: ROMMON_UPG_START (1) INFO: Reset code:
0x00000008 Active ROMMON: Preferred 0, selected 0, booted 0 Firmware upgrade step 2... Detected
current rommon upgrade is available, continue rommon upgrade process Rommon upgrade reset 0 in
progress Reloading now as step 2 of the rommon upgrade process... Rom image verified correctly
Cisco Systems ROMMON, Version 1.1.8, RELEASE SOFTWARE Copyright (c) 1994-2015 by Cisco Systems,
Inc. Compiled Thu 06/18/2015 12:15:56.43 by builders Current image running: *Upgrade in
progress* Boot ROM1 Last reset cause: BootRomUpgrade DIMM Slot 0 : Present DIMM Slot 1 : Present
INFO: Rommon upgrade state: ROMMON_UPG_START (1) INFO: Reset code: 0x00000010 PROM B: stopping
boot timer Active ROMMON: Preferred 0, selected 0, booted 1 INFO: Rommon upgrade state:
ROMMON_UPG_TEST !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!
Please manually or auto boot ASAOS now to complete firmware upgrade !!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Platform ASA5508 with
8192 Mbytes of main memory MAC Address: 18:8b:9d:1e:ca:7c Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately. Located '.boot_string' @ cluster 859024. # Attempt
autoboot: "boot disk0:/asa952-lfbff-k8.SPA" Located 'asa952-lfbff-k8.SPA' @ cluster 818273.
#####
#####
#####
#####
#####
#####
#####
#####
#####
##### LFBFF signature verified. INIT: version 2.88 booting
Starting udev Configuring network interfaces... done. Populating dev cache dosfsck 2.11, 12 Mar
2005, FAT32, LFN There are differences between boot sector and its backup. Differences:
(offset:original/backup) 65:01/00 Not automatically fixing this. Starting check/repair pass.
/cscocofig "." is missing. Can't fix this yet. /cscocofig "." is missing. Can't fix this
yet. Starting verification pass. /cscocofig "." is missing. Can't fix this yet. /cscocofig
"." is missing. Can't fix this yet. /dev/sdb1: 182 files, 849380/1918808 clusters
dosfsck(/dev/sdb1) returned 0 IO Memory Nodes: 1 IO Memory Per Node: 499122176 bytes Global
Reserve Memory Per Node: 314572800 bytes Nodes=1 Processor memory 3807834603 LCMB: got 499122176
bytes on numa-id=0, phys=0x1b8000000, virt=0x2aaaaae00000 LCMB: HEAP-CACHE POOL got 314572800
bytes on numa-id=0, virt=0x2aaac8a00000 Compiled on Sat 28-Nov-15 00:16 PST by builders Total
NICs found: 13 i354 rev03 Gigabit Ethernet @ irq255 dev 20 index 08 MAC: 188b.9d1e.ca7c ivshmem
rev03 Backplane Data Interface @ index 09 MAC: 0000.0001.0002 en_vtun rev00 Backplane Control
Interface @ index 10 MAC: 0000.0001.0001 en_vtun rev00 Backplane Int-Mgmt Interface @ index 11
MAC: 0000.0001.0003 en_vtun rev00 Backplane Ext-Mgmt Interface @ index 12 MAC: 0000.0000.0000
Rom-monitor was successfully upgraded. ...
```

## 확인

‘show module’ 명령을 사용하여 ROMMON 소프트웨어 버전을 확인할 수 있습니다.

```
FTD5508X> enable Password: FTD5508X# show module Mod Card Type Model Serial No. ----
-----
----- 1 ASA 5508-X with FirePOWER
services, 8GE, AC, ASA5508 JAD192100SZ sfr FirePOWER Services Software Module ASA5508
JAD192100SZ Mod MAC Address Range Hw Version Fw Version Sw Version ----
-----
----- 1 188b.9d1e.ca7c to 188b.9d1e.ca84 1.0 1.1.8
9.5(2) sfr 188b.9d1e.ca7b to 188b.9d1e.ca7b N/A N/A 5.4.1-211
```

## 작업 3 - ASA55xx-X에 FTD 부트 이미지 설치

### 작업 요건

ASA5508-X에 FTD 부트 이미지 ftd-boot-9.6.1.0.lfbff를 설치합니다.

### 해결책

여러 가지 방법으로 부트 이미지를 설치할 수 있습니다. 첫 번째 방법은 다음과 같습니다.



```
dosfsck 2.11, 12 Mar 2005, FAT32, LFN
/dev/sdb1: 47 files, 24618/1919063 clusters =====
Launching boot CLI ... Configuring network interface using static IP Bringing up network
interface. Depending on your network, this might take a couple of minutes when using DHCP...
ifup: interface lo already configured Using IPv4 address: 10.62.148.62
Using IPv6 address: fe80::1a8b:9dff:fe1e:ca7b
Using DNS server: 10.62.145.72
Using default gateway: 10.62.148.100
INIT: Starting system message bus: dbus.
Starting OpenBSD Secure Shell server: sshd
generating ssh RSA key...
generating ssh ECDSA key...
generating ssh DSA key...
done.
Starting Advanced Configuration and Power Interface daemon: acpid.
acpid: starting up

acpid: 1 rule loaded

acpid: waiting for events: event logging is off

Starting ntpd: done
Starting syslog-ng:.
Starting crond: OK
```

```
Cisco FTD Boot 6.0.0 (9.6.1.)
Type ? for list of commands
```

```
firepower-boot>
```

ASA5512/15/25/45/55의 구성 절차는 동일하며 부트 이미지 이름만 다릅니다.

```
rommon #0> ADDRESS=10.62.148.10 rommon #1> SERVER=10.229.22.42 rommon #2> GATEWAY=10.62.148.1
rommon #3> IMAGE=ftd-boot-9.6.1.0.cdisk
```

## 방법 2 - ASA 모드에서

### 1단계

ASA 실행 모드(ROMMON 없음)에서 FTD 부트 이미지를 ASA 플래시에 복사합니다.

```
ciscoasa# copy ftp://10.48.40.70/ANG/mzafeiro/ftd-boot-9.6.1.0.lfbff flash
```

### 2단계

디스크에서 모든 ASA 이미지를 삭제합니다.

```
ciscoasa# delete flash:asa*
```

ASA 이미지를 삭제한 후의 플래시 콘텐츠는 다음과 같습니다.

```
ciscoasa# show flash --#-- --length-- -----date/time----- path 131 33 May 20 2016 09:27:28
.boot_string 11 4096 Mar 03 2016 11:48:34 log 154 16767 May 20 2016 09:23:48 log/asa-
appagent.log 155 465 Mar 03 2016 11:54:58 log/asa-ssp_ntp.log 21 4096 Jun 10 2015 06:45:42
crypto_archive 22 4096 Jun 10 2015 06:46:00 coredumpinfo 23 59 Jun 10 2015 06:46:00
coredumpinfo/coredump.cfg 134 25627616 Dec 01 2015 04:01:58 asdm-752.bin 135 52563 Feb 09 2016
02:49:58 system.cfg 136 25028660 Feb 09 2016 02:50:28 asdm-751-112.bin 137 38409858 Feb 09 2016
02:51:14 anyconnect-win-3.1.10010-k9.pkg 138 25629676 Feb 09 2016 04:38:10 asdm-752-153.bin 151
100308208 May 20 2016 09:39:57 ftd-boot-9.6.1.0.lfbff <--
```

### 3단계

ASA를 다시 로드합니다. ASA는 FTD 부트 이미지에서 부팅되어야 합니다.

```
Located 'ftd-boot-9.6.1.0.lfbff' @ cluster 45093.
```

```
##### .. LFBFF signature
```

verified. INIT: version 2.88 booting .. Cisco FTD Boot 6.0.0 (9.6.1.) Type ? for list of commands **firepower-boot>**

## 작업 4 - ASA55xx-X에 FTD 시스템 이미지 설치

ASA5508-X에 FTD 시스템 이미지를 설치합니다.

### 해결책

```
firepower-boot> setup Welcome to Cisco FTD Setup [hit Ctrl-C to abort] Default values are inside
[] Enter a hostname [firepower]: FTD5508 Do you want to configure IPv4 address on management
interface?(y/n) [Y]:
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [Y]: N
Enter an IPv4 address: 10.62.148.29
Enter the netmask: 255.255.255.128
Enter the gateway: 10.62.148.1
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [N]: Enter
an IPv4 address [10.62.148.29]: Enter the netmask [255.255.255.128]: Enter the gateway
[10.62.148.1]: Do you want to configure static IPv6 address on management interface?(y/n) [N]:
Stateless autoconfiguration will be enabled for IPv6 addresses. Enter the primary DNS server IP
address: 173.38.200.100 Do you want to configure Secondary DNS Server? (y/n) [n]: y Enter the
secondary DNS server IP address: 144.254.71.184 Do you want to configure Local Domain Name?
(y/n) [n]: Do you want to configure Search domains? (y/n) [n]: Do you want to enable the NTP
service? [Y]: Enter the NTP servers separated by commas [203.0.113.126]: 171.68.38.65 Please
review the final configuration: Hostname: FTD5508 Management Interface Configuration IPv4
Configuration: static IP Address: 10.62.148.29 Netmask: 255.255.255.128 Gateway: 10.62.148.1
IPv6 Configuration: Stateless autoconfiguration DNS Configuration: DNS Server: 173.38.200.100
144.254.71.184 NTP configuration: 171.68.38.65 CAUTION: You have selected IPv6 stateless
autoconfiguration, which assigns a global address based on network prefix and a device
identifier. Although this address is unlikely to change, if it does change, the system will stop
functioning correctly. We suggest you use static addressing instead. Apply the changes?(y,n)
[Y]: Configuration saved successfully! Applying... Done. Press ENTER to continue... firepower-
boot>
```

FTP 서버와의 연결을 확인합니다.

```
firepower-boot> ping 10.229.22.42
PING 10.229.22.42 (10.229.22.42) 56(84) bytes of data.
64 bytes from 10.229.22.42: icmp_seq=1 ttl=124 time=1.30 ms
64 bytes from 10.229.22.42: icmp_seq=2 ttl=124 time=1.32 ms
64 bytes from 10.229.22.42: icmp_seq=3 ttl=124 time=1.45 ms
^C
--- 10.229.22.42 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.302/1.360/1.458/0.075 ms
```

시스템 패키지를 설치합니다.

```
firepower-boot> system install ftp://10.229.22.42/ftd-6.0.0-1005.pkg #####
WARNING ##### # The content of disk0: will be erased during installation!
# ##### Do you want to continue? [y/N] y
Erasing disk0 ... Verifying Enter credentials to authenticate with ftp server Username: ftp
Password: Verifying Downloading Extracting <-- Here give it some time (~10 min) Package Detail
Description: Cisco ASA-NGFW 6.0.0-1005 System Install Requires reboot: Yes Do you want to
continue with upgrade? [y]: <-- Press Enter Warning: Please do not interrupt the process or turn
off the system. Doing so might leave system in unusable state. Starting upgrade process ...
Populating new system image <-- Here give it some time (~5 min) Reboot is required to complete
the upgrade. Press 'Enter' to reboot the system. <-- Press Enter Broadcast message from
root@firepowStopping OpenBSD Secure Shell server: sshdstopped /usr/sbin/sshd (pid 1963) .
Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid (pid 1967)
acpid: exiting acpid. Stopping system message bus: dbus. Stopping ntpd: stopped process in
pidfile '/var/run/ntp.pid' (pid 2055) done Stopping crond: OK Deconfiguring network
interfaces... done. Sending all processes the TERM signal... Sending all processes the KILL
```



signal... Deactivating swap... Unmounting local filesystems... Rebooting... y Rom image verified correctly Cisco Systems ROMMON, Version 1.1.8, RELEASE SOFTWARE Copyright (c) 1994-2015 by Cisco Systems, Inc. Compiled Thu 06/18/2015 12:15:56.43 by builders Current image running: Boot ROM1 Last reset cause: PowerCycleRequest DIMM Slot 0 : Present DIMM Slot 1 : Present Platform ASA5508 with 8192 Mbytes of main memory MAC Address: 18:8b:9d:1e:ca:7c Use BREAK or ESC to interrupt boot. Use SPACE to begin boot immediately. Located '.boot\_string' @ cluster 186016. # Attempt autoboot: "boot disk0:os.img" Located 'os.img' @ cluster 160001.

##### LFBFF signature verified. INIT: version 2.88 booting Starting udev Configuring network interfaces... done. Populating dev cache Detected PID ASA5508. Found device serial number JAD192100SZ. Found USB flash drive /dev/sdb Found hard drive(s): /dev/sda fsck from util-linux 2.23.2 dosfsck 2.11, 12 Mar 2005, FAT32, LFN /dev/sdb1: 7 files, 26064/1919063 clusters ===== Use ESC to interrupt boot and launch boot CLI. Use SPACE to launch Cisco FTD immediately. Cisco FTD launch in 20 seconds ... Running on kenton Mounting disk partitions ... Initializing Threat Defense ... [ OK ] Starting system log daemon... [ OK ] Flushing all current IPv4 rules and user defined chains: ...success Clearing all current IPv4 rules and user defined chains: ...success Applying iptables firewall rules: Flushing chain `PREROUTING' Flushing chain `INPUT' Flushing chain `FORWARD' Flushing chain `OUTPUT' Flushing chain `POSTROUTING' Flushing chain `INPUT' Flushing chain `FORWARD' Flushing chain `OUTPUT' Applying rules succeeded Flushing all current IPv6 rules and user defined chains: ...success Clearing all current IPv6 rules and user defined chains: ...success Applying ip6tables firewall rules: Flushing chain `PREROUTING' Flushing chain `INPUT' Flushing chain `FORWARD' Flushing chain `OUTPUT' Flushing chain `POSTROUTING' Flushing chain `INPUT' Flushing chain `FORWARD' Flushing chain `OUTPUT' Applying rules succeeded Starting nscd... mkdir: created directory '/var/run/nscd' [ OK ] Starting , please wait...grep: /ngfw/etc/motd: No such file or directory ...complete. Firstboot detected, executing scripts Executing S01reset\_failopen\_if [ OK ] Executing S04fix-httpd.sh [ OK ] Executing S05set-mgmt-port [ OK ] Executing S06addusers [ OK ] Executing S07uuid-init [ OK ] Executing S09configure\_mysql [ OK ] \*\*\*\*\* Attention \*\*\*\*\* Initializing the configuration database. Depending on available system resources (CPU, memory, and disk), this may take 30 minutes or more to complete. \*\*\*\*\* Attention \*\*\*\*\* Executing S10database [ OK ] Executing S12install\_infodb [ OK ] Executing S15set-locale.sh [ OK ] Executing S16update-sensor.pl [ OK ] Executing S19cert-tun-init [ OK ] Executing S20cert-init [ OK ] Executing S21disable\_estreamer [ OK ] Executing S25create\_default\_des.pl [ OK ] Executing S30init\_lights\_out\_mgmt.pl [ OK ] Executing S40install\_default\_filters.pl [ OK ] Executing S42install\_default\_dashboards.pl [ OK ] Executing S43install\_default\_report\_templates.pl [ OK ] Executing S44install\_default\_app\_filters.pl [ OK ] Executing S45install\_default\_realms.pl [ OK ] Executing S47install\_default\_sandbox\_EO.pl [ OK ] Executing S50install-remediation-modules [ OK ] Executing S51install\_health\_policy.pl [ OK ] Executing S52install\_system\_policy.pl [ OK ] Executing S53change\_reconciliation\_baseline.pl [ OK ] Executing S70update\_sensor\_objects.sh [ OK ] Executing S85patch\_history-init [ OK ] Executing S90banner-init [ OK ] Executing S95copy-crontab [ OK ] Executing S96grow\_var.sh [ OK ] \*\*\*\*\* Attention \*\*\*\*\* Initializing the system's localization settings. Depending on available system resources (CPU, memory, and disk), this may take 10 minutes or more to complete. \*\*\*\*\* Attention \*\*\*\*\* Executing S96localize-templates [ OK ] Executing S96ovf-data.pl [ OK ] Executing S97compress-client-resources [ OK ] Executing S97create\_platinum\_forms.pl [ OK ] Executing S97install\_cloud\_support.pl [ OK ] Executing S97install\_geolocation.pl [ OK ] Executing S97install\_ssl\_inspection.pl [ OK ] Executing S97update\_modprobe.pl [ OK ] Executing S98check-db-integrity.sh [ OK ] Executing S98htaccess-init [ OK ] Executing S99correct\_ipmi.pl [ OK ] Executing S99start-system [ OK ] Executing S99z\_db\_restore [ OK ] Firstboot scripts finished. Configuring NTP... [ OK ] Model reconfigure detected, executing scripts Pinging mysql Found mysql is running Executing 45update-sensor.pl [ OK ] Executing 55recalculate\_arc.pl [ OK ] Starting xinetd: Mon Mar 14 18:28:11 UTC 2016 Starting MySQL... Pinging mysql Pinging mysql, try 1 Found mysql is running Running initializeObjects... Stopping MySQL... Killing mysqld with pid 10993 Wait for mysqld to exit\c done Mon Mar 14 18:28:21 UTC 2016 Starting sfid... [ OK ] Starting Cisco ASA5508-X Threat Defense, please wait...No PM running! ...started. INIT: Starting system message bus: dbus. Starting OpenBSD Secure Shell server: sshd generating ssh RSA key... generating ssh ECDSA key... generating ssh DSA key... done. Starting Advanced Configuration and Power Interface daemon: acpid. Starting crond: OK Mar 14 18:28:26 ciscoasa SF-IMS[11490]: [11490] init script:system [INFO] pmmon Setting affinity to 5-7... pid 11486's current affinity list: 0-7 pid 11486's new affinity list: 5-7 Mar 14 18:28:26 ciscoasa SF-IMS[11492]: [11492] init script:system [INFO] pmmon The Process Manager is not running... Mar 14 18:28:26 ciscoasa SF-IMS[11493]: [11493] init script:system [INFO] pmmon Starting the Process Manager... Mar 14 18:28:26 ciscoasa SF-IMS[11494]: [11494] pm:pm [INFO] Using model number 75K Cisco ASA5508-X Threat Defense v6.0.0 (build 1005) ciscoasa login: Compiled on Sat 07-Nov-15 16:13 PST by

```
builders Total NICs found: 13 i354 rev03 Gigabit Ethernet @ irq255 dev 20 index 08 MAC:
188b.9d1e.ca7c ivshmem rev03 Backplane Data Interface @ index 09 MAC: 0000.0001.0002 en_vtun
rev00 Backplane Control Interface @ index 10 MAC: 0000.0001.0001 en_vtun rev00 Backplane Int-
Mgmt Interface @ index 11 MAC: 0000.0001.0003 en_vtun rev00 Backplane Ext-Mgmt Interface @ index
12 MAC: 0000.0000.0000 INFO: Unable to read firewall mode from flash Writing default firewall
mode (single) to flash INFO: Unable to read cluster interface-mode from flash Writing default
mode "None" to flash Verify the activation-key, it might take a while... Failed to retrieve
permanent activation key. Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 The Running Activation Key is not valid, using default settings: Licensed
features for this platform: Maximum Physical Interfaces : Unlimited perpetual Maximum VLANs : 50
perpetual Inside Hosts : Unlimited perpetual Failover : Active/Active perpetual Encryption-DES :
Enabled perpetual Encryption-3DES-AES : Disabled perpetual Security Contexts : 2 perpetual
GTP/GPRS : Disabled perpetual AnyConnect Premium Peers : 4 perpetual AnyConnect Essentials :
Disabled perpetual Other VPN Peers : 100 perpetual Total VPN Peers : 100 perpetual Shared
License : Disabled perpetual AnyConnect for Mobile : Disabled perpetual AnyConnect for Cisco VPN
Phone : Disabled perpetual Advanced Endpoint Assessment : Disabled perpetual Total UC Proxy
Sessions : 320 perpetual Botnet Traffic Filter : Disabled perpetual Cluster : Disabled perpetual
VPN Load Balancing : Enabled perpetual Encryption hardware device : Cisco ASA Crypto on-board
accelerator (revision 0x1) Cisco Adaptive Security Appliance Software Version 99.1(3)194
***** Warning ***** This product contains
cryptographic features and is subject to United States and local country laws governing, import,
export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party
authority to import, export, distribute, or use encryption. Importers, exporters, distributors
and users are responsible for compliance with U.S. and local country laws. By using this product
you agree to comply with applicable laws and regulations. If you are unable to comply with U.S.
and local laws, return the enclosed items immediately. A summary of U.S. laws governing Cisco
cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
***** Warning ***** ... output omitted ...
Reading from flash... ! Cryptochecksum (changed): 6129864f 6298b553 75f279ea e547792b INFO:
Power-On Self-Test in process. .... INFO: Power-On Self-Test complete. INFO:
Starting HW-DRBG health test... INFO: HW-DRBG health test passed. INFO: Starting SW-DRBG health
test... INFO: SW-DRBG health test passed. Cisco ASA5508-X Threat Defense v6.0.0 (build 1005)
firepower login: admin Password: <-- Admin123 You must accept the EULA to continue. Press
<ENTER> to display the EULA:
... EULA is displayed - output is omitted END USER LICENSE AGREEMENT Please enter 'YES' or press
to AGREE to the EULA: System initialization in progress. Please stand by. You must change the
password for 'admin' to continue. Enter new password: Confirm new password: You must configure
the network to continue. You must configure at least one of IPv4 or IPv6. Do you want to
configure IPv4? (y/n) [y]: Do you want to configure IPv6? (y/n) [n]: Configure IPv4 via DHCP or
manually? (dhcp/manual) [manual]: Enter an IPv4 address for the management interface
[192.168.45.45]: 10.62.148.29 Enter an IPv4 netmask for the management interface
[255.255.255.0]: 255.255.255.128 Enter the IPv4 default gateway for the management interface []:
10.62.148.1 Enter a fully qualified hostname for this system [firepower]: FTD5508 Enter a comma-
separated list of DNS servers or 'none' []: 173.38.200.100,144.254.71.184 Enter a comma-
separated list of search domains or 'none' []: If your networking information has changed, you
will need to reconnect. For HTTP Proxy configuration, run 'configure network http-proxy'
Configure firewall mode? (routed/transparent) [routed]: Configuring firewall mode ... Update
policy deployment information - add device configuration You can register the sensor to a
Firepower Management Center and use the Firepower Management Center to manage it. Note that
registering the sensor to a Firepower Management Center disables on-sensor Firepower Services
management capabilities. When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required. In most cases, to register a sensor to a
Firepower Management Center, you must provide the hostname or the IP address along with the
registration key. 'configure manager add [hostname | ip address ] [registration key ]' However,
if the sensor and the Firepower Management Center are separated by a NAT device, you must enter
a unique NAT ID, along with the unique registration key. 'configure manager add DONTRESOLVE
[registration key ] [ NAT ID ]' Later, using the web interface on the Firepower Management
Center, you must use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center. >
```

**팁: 'noconfirm' 옵션을 사용하여 이미지를 설치할 수 있습니다. 이 경우 설치 중에 프롬프트가 표시되지 않습니다.**

```
firepower-boot>system install noconfirm ftp://10.229.22.42/ftd-6.0.0-1005.pkg
```

FTD 6.1.x 이상 버전에서는 관리 모드(로컬 또는 원격)를 지정하라는 프롬프트가 표시됩니다.

For HTTP Proxy configuration, run 'configure network http-proxy'

```
Manage the device locally? (yes/no) [yes]: no Configure firewall mode? (routed/transparent)
[routed]:
```

로컬 모드 = ASA55xx-X 디바이스에만 해당됩니다. FDM(Firepower Device Manager)에서 FTD를 관리합니다.

원격 모드 = FMC(Firepower Management Center)에서 FTD를 관리합니다.

### 확인

```
> show version -----[ FTD5508 ]----- Model : Cisco ASA5508-X Threat
Defense (75) Version 6.0.0 (Build 1005) UUID : 8c3f4b7e-ea11-11e5-94f1-f3a55afb51a3 Rules update
version : 2015-10-01-001-vrt VDB version : 252 -----
--- >
```

ASA5512/15/25/45/55에 시스템 이미지 설치 과정도 위 내용과 동일합니다.

## 작업 5 - FMC에 FTD 등록

다음 설정을 사용하여 FMC 서버에 FTD를 등록합니다.

Host	10.62.148.29
표시 이름	FTD5508
등록 키	cisco
Group None(그룹 없음)	
액세스 제어 정책	FTD5508
Access Control Policy Base Policy(액세스 제어 정책 기준 정책)	없음
Access Control Policy Default Action(액세스 제어 정책 기본 작업)	Block all Traffic(모든 트래픽 차단)

### 해결책

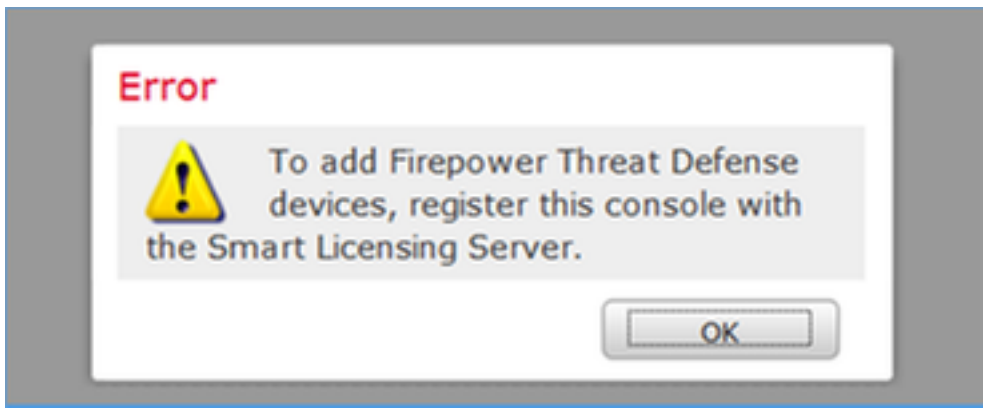
#### 1단계

FTD에서 FMC 서버를 지정합니다.

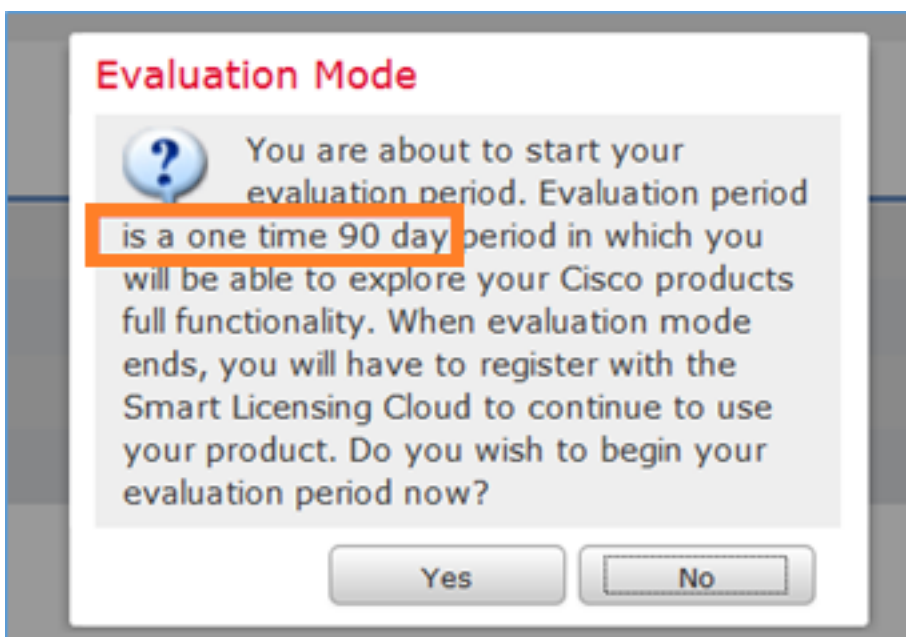
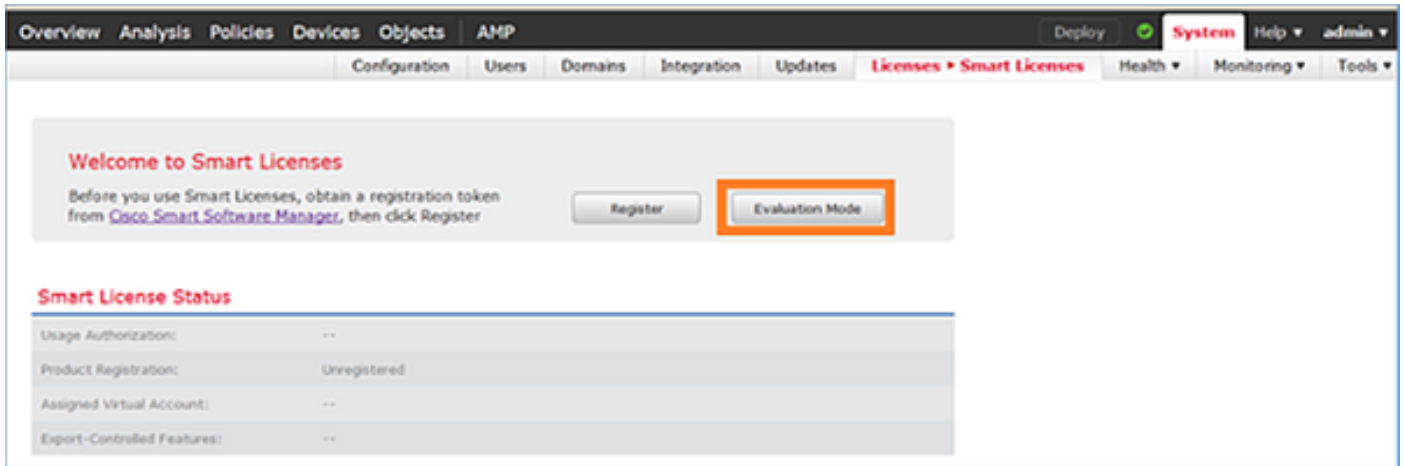
```
> configure manager add 10.62.148.73 cisco Manager successfully configured. Please make note of
reg_key as this will be required while adding Device in FMC. > show managers Host : 10.62.148.73
Registration Key : **** Registration : pending RPC Status : Type : Manager Host : 10.62.148.73
Registration : Pending >
```

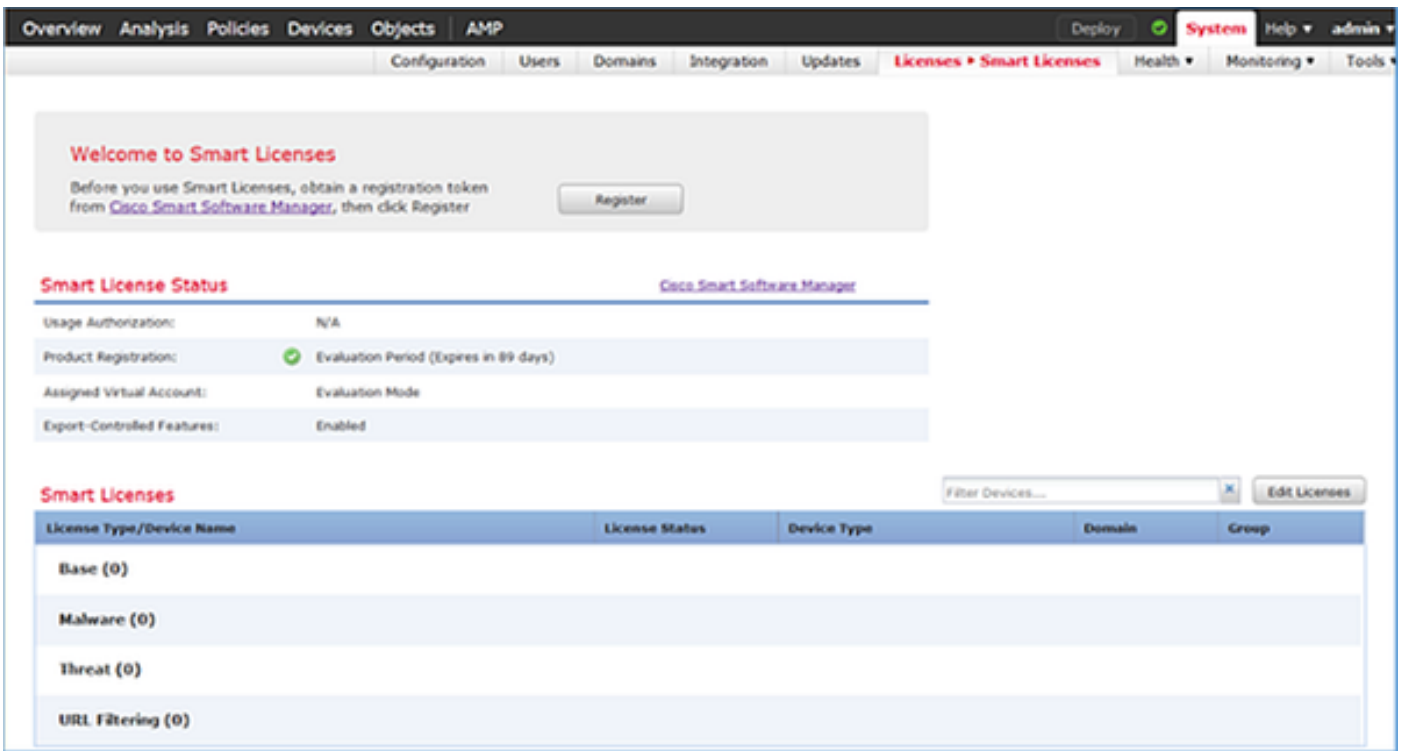
#### 2단계

FTD를 추가하기 전에 스마트 라이선싱 서버에 FMC를 등록해야 합니다. 스마트 라이선스 없이 FTD 디바이스를 추가하려고 하면 다음 오류가 발생합니다.



평가 모드를 선택할 수 있습니다. 이렇게 하면 90일 동안 FTD를 사용할 수 있습니다.

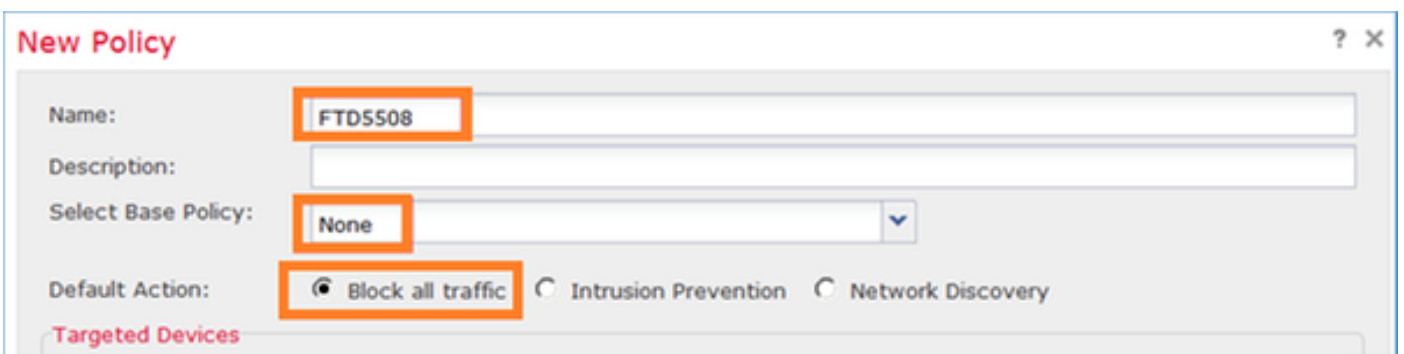
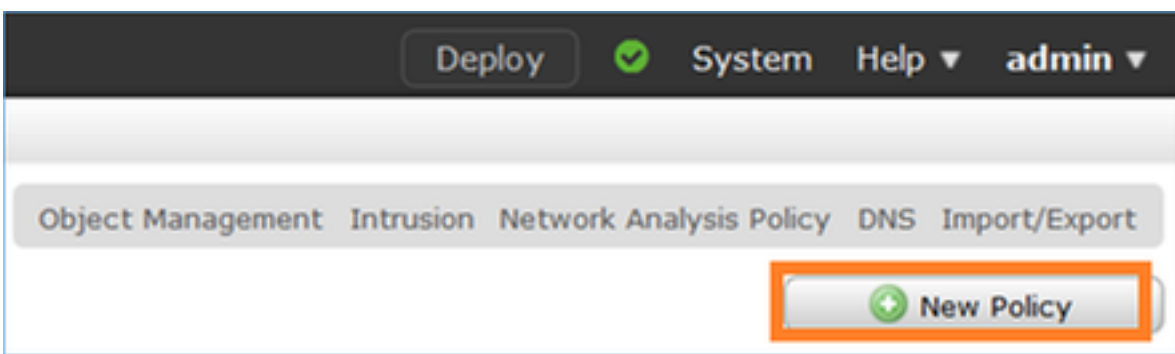
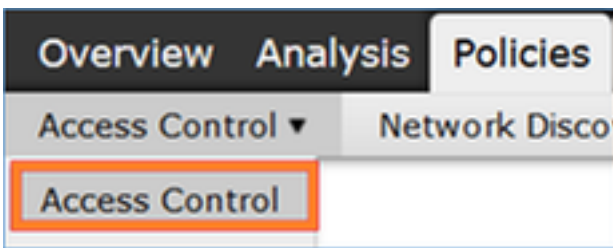




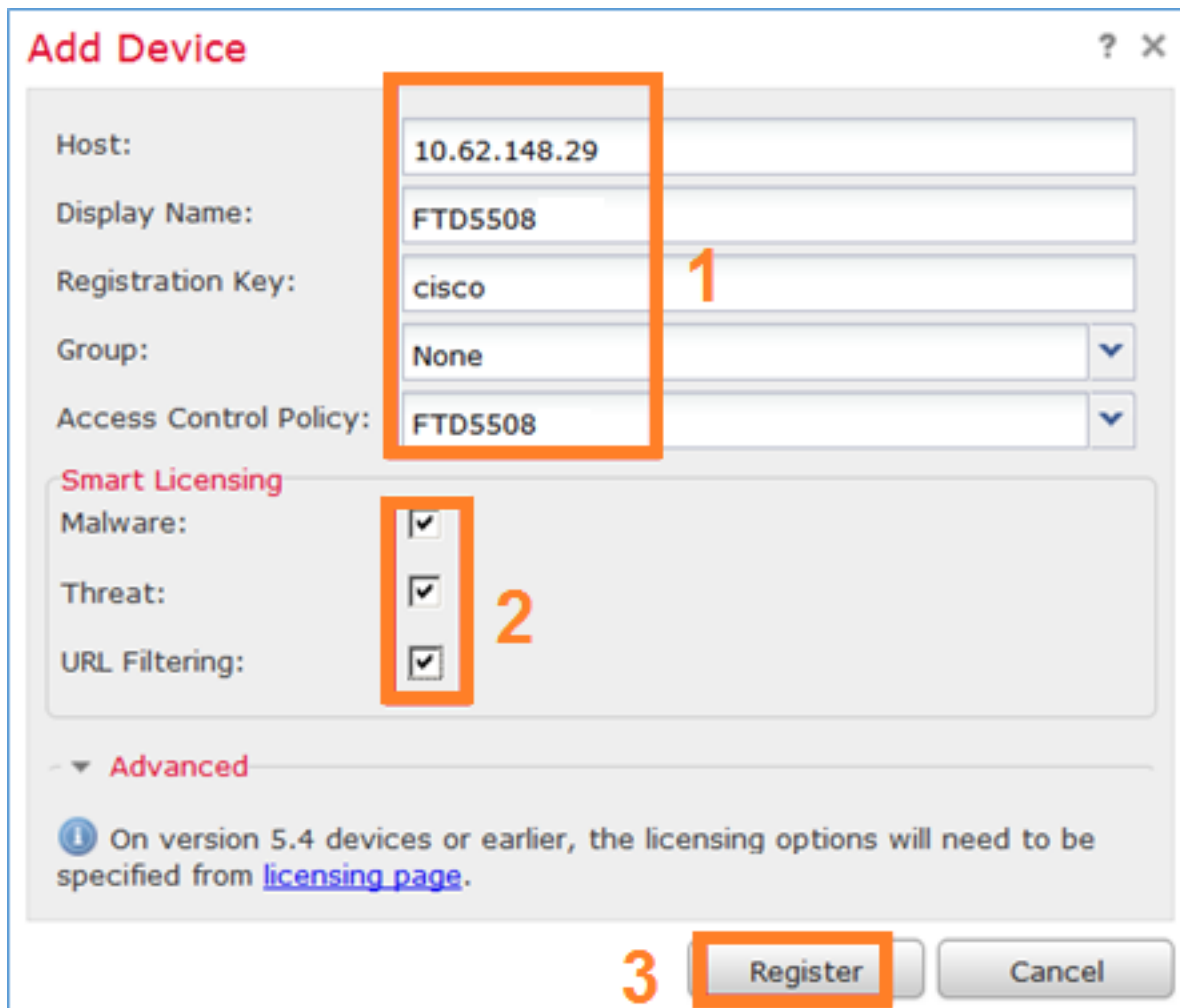
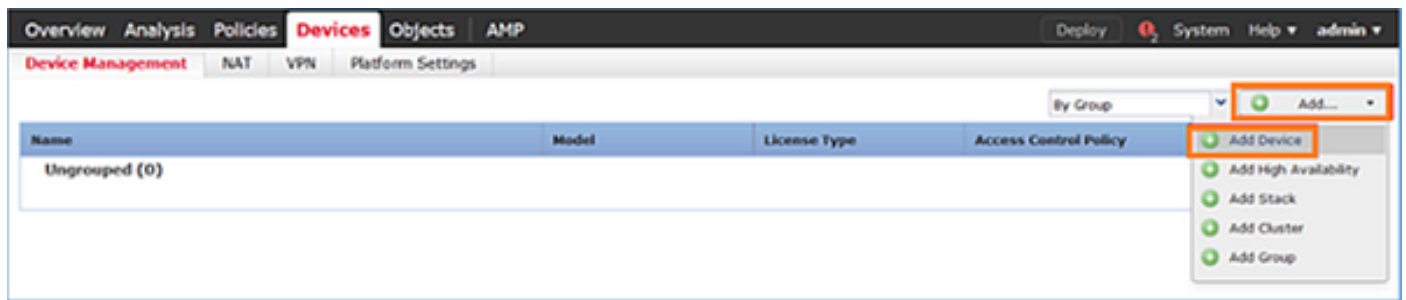
### 3단계

먼저 FMC에서 FTD가 사용하도록 할 액세스 제어 정책을 생성합니다.

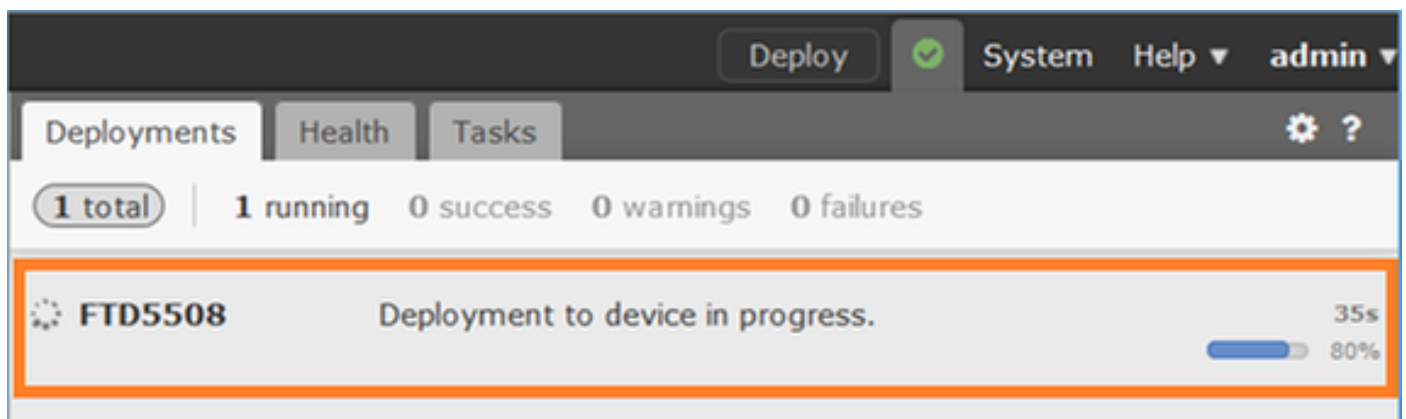
Policies(정책) > Access Control(액세스 제어)로 이동하여 New Policy(새 정책)를 클릭합니다.



그런 다음 FTD 디바이스를 추가합니다.



FTD 추가가 완료되면 정책이 구축됩니다.



FTD 디바이스를 추가하는 동안 백그라운드에서 수행되는 작업을 확인하려면 FMC와 FTD 둘 다에서 **pigtail**을 활성화합니다.

## FMC의 경우:

```
admin@fs4k:~$ sudo pigtail
*****
***** ** Displaying logs: ACTQ HTTP DCSM VMSS MOJO NGFW NGUI VMSB TCAT
DEPL MSGS USMS
*****
*****
```

## FTD의 경우:

```
> pigtail ***** **
Displaying logs: HTTP ACTQ DCSM VMSS MOJO NGUI NGFW TCAT VMSB DEPL USMS MSGS
*****
```

트러블슈팅 관련 참고 사항 - FTD 관리 인터페이스 상태가 “down(다운)”이면 confreg 값이 “0x1”인지 확인합니다.

# 작업 6 - FTD 업그레이드

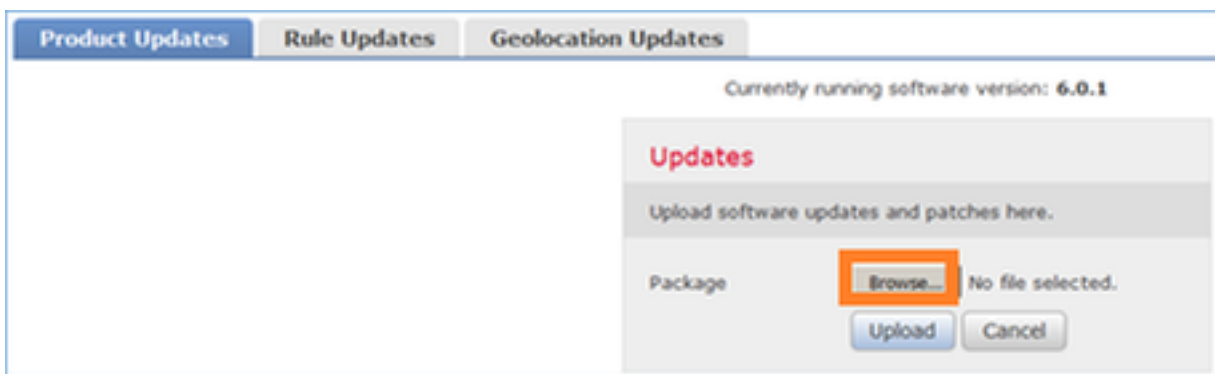
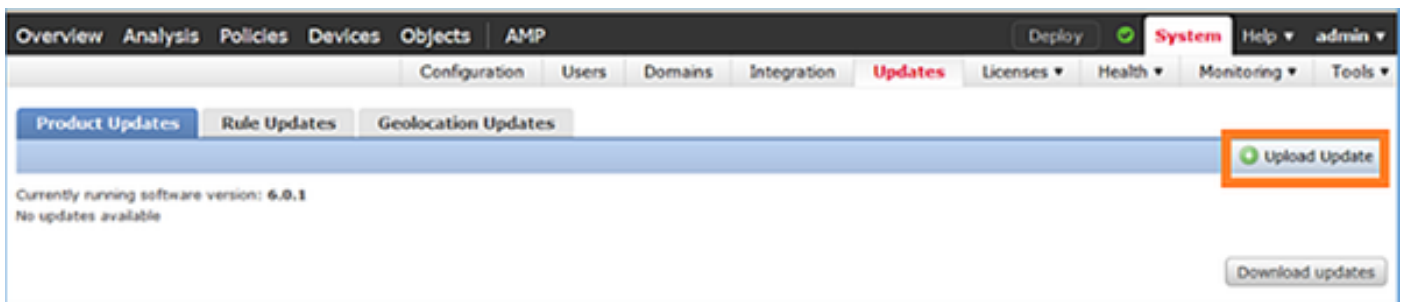
이 작업에서는 FTD를 6.0.0에서 6.0.1로 업그레이드합니다.

	버전	파일 이름
초기 FTD 이미지	버전 6.0.0(빌드 1005)	ftd-6.0.0-1005.pkg
타겟 FTD 이미지	버전 6.0.1(빌드 1213)	Cisco_FTD_Upgrade-6.0.1-1213.sh

## 해결책

### 1단계

FMC에 FTD 이미지를 업로드합니다.



### 2단계

FTD 이미지를 설치합니다.

The screenshot shows the Cisco FTD management console interface. At the top, there are navigation tabs: Overview, Analysis, Policies, Devices, Objects, AMP, and System. Below these are sub-tabs: Configuration, Users, Domains, Integration, Updates, Licenses, Health, Monitoring, and Tools. The 'Updates' sub-tab is active, showing 'Product Updates', 'Rule Updates', and 'Geolocation Updates'. A 'Task Notification' box displays a success message: 'Message\_Center\_Tasks\_Tab Your task Installing Sourcefire Geolocation Database Update version: GeoDB-2016-03-05-001 (Local Install) succeeded at Wed Mar 23 11:52:57 2016. Successfully installed the Geolocation Database'. Below this is a green 'Success' box: 'Upload succeeded'. The current software version is 6.0.1. A table lists updates:

Type	Version	Date	Release Notes	Reboot
Cisco FTD Upgrade	6.0.1-1213	Sat Mar 19 01:41:15 UTC 2016		Yes

The screenshot shows the 'Selected Update' details for the Cisco FTD Upgrade. The details are:

- Type: Cisco FTD Upgrade
- Version: 6.0.1-1213
- Date: Sat Mar 19 01:41:15 UTC 2016
- Release Notes:
- Reboot: Yes

Below the details, there is a list of updates under the heading 'Ungrouped (1 total)'. The first update is selected and highlighted with a red box and the number '1':

ID	Name	Health Policy
FTD5508	10.62.148.29 - Cisco ASA5508-X Threat Defense v6.0.0	None

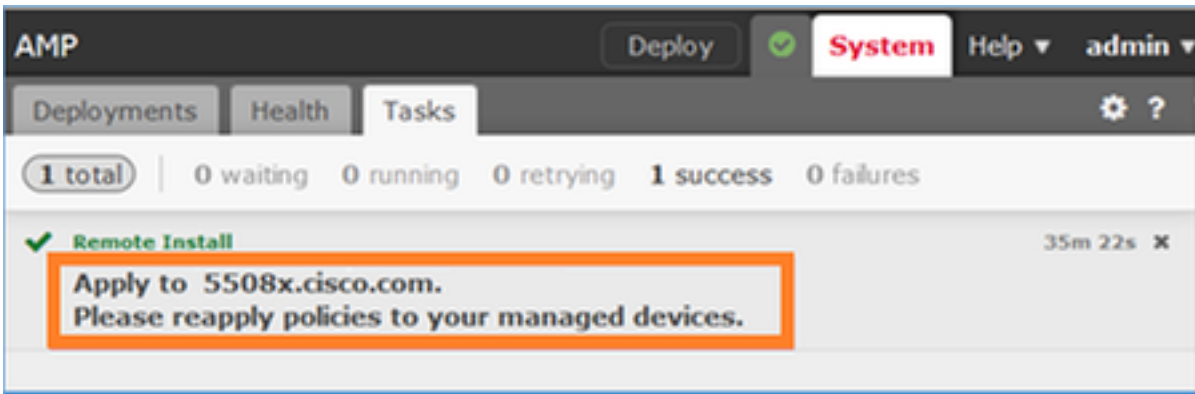
At the bottom right, there is an 'Install' button highlighted with a red box and the number '2', and a 'Cancel' button next to it.

FTD 다시 로드에 대한 경고가 표시됩니다.

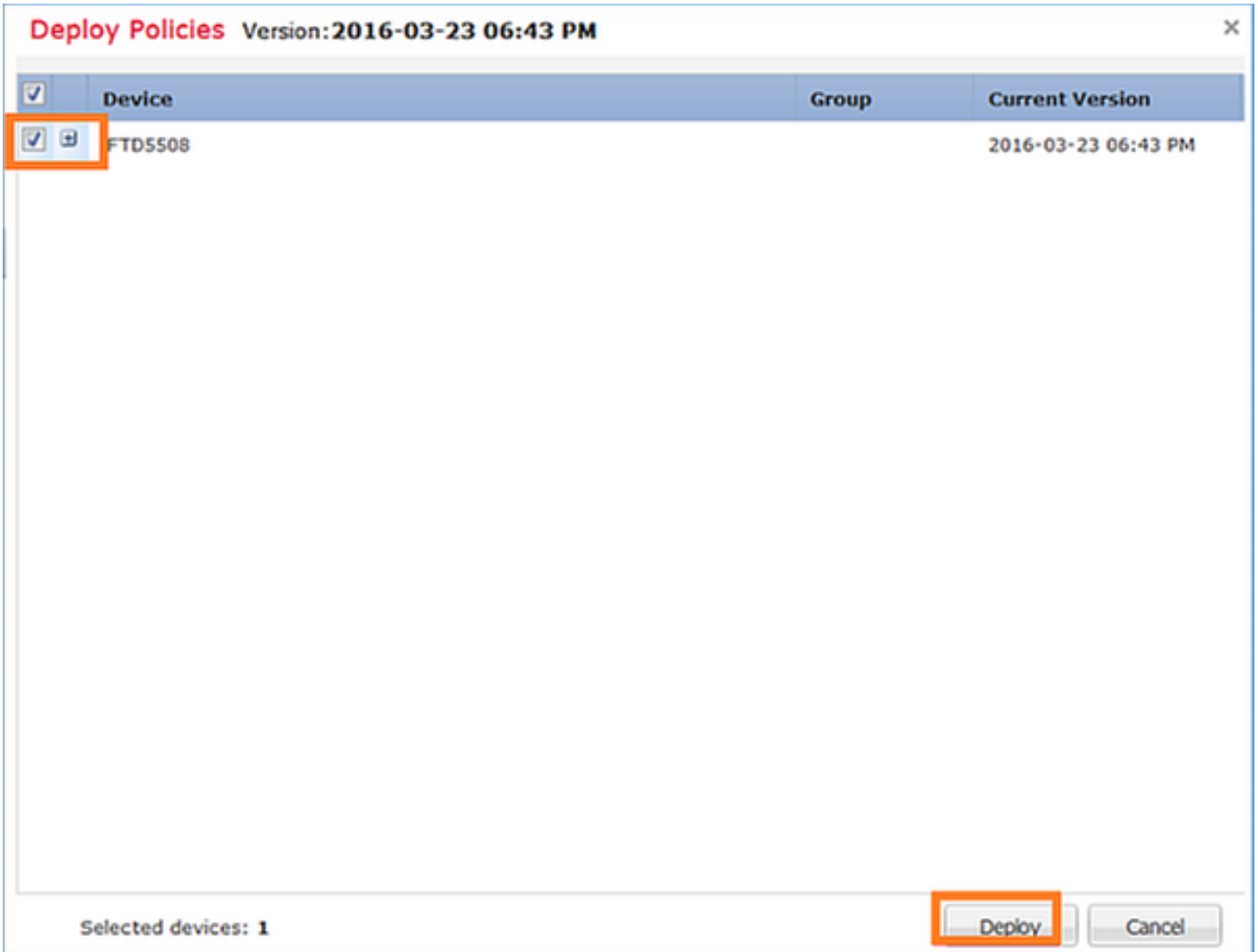
The screenshot shows a warning dialog box with the text: 'Update installation will reboot the system(s). Are you sure you want to continue?'. At the bottom, there are two buttons: 'OK' and 'Cancel'.

이 예에서는 업그레이드에 35분 정도가 걸렸습니다. 아래에 나와 있는 것처럼 정책을 다시 적용해야 합니다.





정책을 구축합니다.



확인

FTD 업그레이드 후:

```
> show version
-----[ FTD5508 ]-----
Model           : Cisco ASA5508-X Threat Defense (75) Version 6.0.1 (Build 1213)
UUID            : 53b44806-f0f4-11e5-88cc-c72c24d24877
Rules update version : 2016-03-04-001-vrt
VDB version     : 259
-----
```

>

## 작업 7 - ASA 엔진 CLI 모드로 진입 및 CLI 모드에서 분리

ASA CLI 모드로 진입한 다음 모드 연결을 끊습니다.

### 해결책

FTD CLISH 모드에서 다음 명령을 입력합니다.

```
> system support diagnostic-cli Attaching to ASA console ... Press 'Ctrl+a then d' to detach.  
Type help or '?' for a list of available commands. firepower>
```

```
firepower> enable Password: <-- by default empty (null) firepower#
```

위의 메시지에 나와 있는 대로, FTD ASA 콘솔에서 연결을 끊으려면(콘솔을 분리하려면) Ctrl+A를 누르고 D 키를 누릅니다.

```
firepower# <- 'Ctrl+a then d' Console connection detached. admin@FTD5508:~$
```

## 작업 8 - 기존 FTD 설치 이미지로 다시 설치

### 요건

기존 FTD 이미지로 다시 설치하고 버전 6.1.0-330을 설치합니다.

### 해결책

이 작업에서는 코드 6.0.1.x를 실행하는 FTD 어플라이언스가 있으며 복구할 수 없는 데이터베이스 손상, 치명적인 결함으로 인한 소프트웨어 업그레이드 불가 등의 이유로 어플라이언스를 이미지로 다시 설치해야 한다고 가정합니다.

### 단계 요약

1. 호환성 검사
2. FMC에서 FTD 등록 취소
3. FTD 어플라이언스를 다시 로드하고 BootCLI 진입
4. 설정 마법사 실행
5. FTD 시스템 이미지 설치
6. FMC에 FTD 등록



```
clusters ===== Use ESC to interrupt boot and launch
boot CLI. Use SPACE to launch Cisco FTD immediately. Cisco FTD launch in 23 seconds ... < Press
ESC to enter BootCLI Launching boot CLI ... Configuring network interface using DHCP Bringing up
network interface. Depending on your network, this might take a couple of minutes when using
DHCP... ifup: interface lo already configured Using IPv6 address: fe80::863d:c6ff:fela:cf38 IPv4
address not assigned. Run 'setup' before installation. INIT: Starting system message bus: dbus.
Starting OpenBSD Secure Shell server: sshd generating ssh RSA key... generating ssh ECDSA key...
generating ssh DSA key... done. Starting Advanced Configuration and Power Interface daemon:
acpid. acpid: starting up acpid: 1 rule loaded acpid: waiting for events: event logging is off
Starting ntpd: done Starting syslog-ng:[2017-01-14T11:20:33.699619] Connection failed; fd='15',
server='AF_INET(127.128.254.1:514)', local='AF_INET(0.0.0.0:0)', error='Network is unreachable
(101)' [2017-01-14T11:20:33.699704] Initiating connection failed, reconnecting; time_reopen='60'
. Starting crond: OK Cisco FTD Boot 6.0.0 (9.6.2.) Type ? for list of commands firepower-boot>
```

## 4단계

설정 마법사를 실행하여 기본 네트워크 파라미터를 설정합니다.

```
firepower-boot>setup Welcome to Cisco FTD Setup [hit Ctrl-C to abort] Default values are inside
[] Enter a hostname [firepower]: FTD5506 Do you want to configure IPv4 address on management
interface?(y/n) [Y]: Y Do you want to enable DHCP for IPv4 address assignment on management
interface?(y/n) [Y]: n Enter an IPv4 address: 10.48.66.83 Enter the netmask: 255.255.255.128
Enter the gateway: 10.48.66.1 Do you want to configure static IPv6 address on management
interface?(y/n) [N]: N Stateless autoconfiguration will be enabled for IPv6 addresses. Enter the
primary DNS server IP address: 192.168.0.1 Do you want to configure Secondary DNS Server? (y/n)
[n]: n Do you want to configure Local Domain Name? (y/n) [n]: n Do you want to configure Search
domains? (y/n) [n]: n Do you want to enable the NTP service? [Y]: n Please review the final
configuration: Hostname: FTD5506 Management Interface Configuration IPv4 Configuration: static
IP Address: 10.48.66.83 Netmask: 255.255.255.128 Gateway: 10.48.66.1 IPv6 Configuration:
Stateless autoconfiguration DNS Configuration: DNS Server: 192.168.0.1 NTP configuration:
Disabled CAUTION: You have selected IPv6 stateless autoconfiguration, which assigns a global
address based on network prefix and a device identifier. Although this address is unlikely to
change, if it does change, the system will stop functioning correctly. We suggest you use static
addressing instead. Apply the changes?(y,n) [Y]: Y Configuration saved successfully! Applying...
Restarting network services... Done. Press ENTER to continue... firepower-boot>
```

## 5단계

FTD 시스템 이미지가 포함된 서버(FTP, HTTP 등)와의 연결을 확인하고 설치를 시작합니다.

```
firepower-boot>ping 10.48.40.70 PING 10.48.40.70 (10.48.40.70) 56(84) bytes of data. 64 bytes
from 10.48.40.70: icmp_seq=1 ttl=64 time=555 ms 64 bytes from 10.48.40.70: icmp_seq=2 ttl=64
time=0.465 ms 64 bytes from 10.48.40.70: icmp_seq=3 ttl=64 time=0.511 ms --- 10.48.40.70 ping
statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2000ms rtt
min/avg/max/mdev = 0.465/185.466/555.424/261.599 ms firepower-boot > system install noconfirm
ftp://anonymous:cisco@10.48.40.70/ftd-6.1.0-330.pkg ##### WARNING
##### # The content of disk0: will be erased during installation! #
##### Do you want to continue? [y/N] y
Erasing disk0 ... Verifying Downloading Extracting Package Detail Description: Cisco ASA-FTD
6.1.0-330 System Install Requires reboot: Yes Warning: Please do not interrupt the process or
turn off the system. Doing so might leave system in unusable state. Starting upgrade process ...
Populating new system image ... output omitted ... Firstboot detected, executing scripts
Executing S01reset_failopen_if [ OK ] Executing S01virtual-machine-reconfigure [ OK ] Executing
S02aws-pull-cfg [ OK ] Executing S02configure_onbox [ OK ] Executing S04fix-httpd.sh [ OK ]
Executing S05set-mgmt-port [ OK ] Executing S06addusers [ OK ] Executing S07uuid-init [ OK ]
Executing S08configure_mysql [ OK ] ***** Attention ***** Initializing the
configuration database. Depending on available system resources (CPU, memory, and disk), this
```

```

may take 30 minutes or more to complete. ***** Attention ***** Executing S09database-
init [ OK ] Executing S11database-populate [ OK ] Executing S12install_infodb [ OK ] Executing
S15set-locale.sh [ OK ] Executing S16update-sensor.pl [ OK ] Executing S19cert-tun-init [ OK ]
Executing S20cert-init [ OK ] Executing S21disable_estreamer [ OK ] Executing
S25create_default_des.pl [ OK ] Executing S30init_lights_out_mgmt.pl [ OK ] Executing
S40install_default_filters.pl [ OK ] Executing S42install_default_dashboards.pl [ OK ] Executing
S43install_default_report_templates.pl [ OK ] Executing S44install_default_app_filters.pl [ OK ]
Executing S45install_default_realms.pl [ OK ] Executing S47install_default_sandbox_EO.pl [ OK ]
Executing S50install-remediation-modules [ OK ] Executing S51install_health_policy.pl [ OK ]
Executing S52install_system_policy.pl [ OK ] Executing S53change_reconciliation_baseline.pl [ OK
] Executing S70remove_casuser.pl [ OK ] Executing S70update_sensor_objects.sh [ OK ] Executing
S85patch_history-init [ OK ] Executing S90banner-init [ OK ] Executing S95copy-crontab [ OK ]
Executing S96grow_var.sh [ OK ] Executing S96install_vmware_tools.pl [ OK ] ***** Attention
***** Initializing the system's localization settings. Depending on available system
resources (CPU, memory, and disk), this may take 10 minutes or more to complete. *****
Attention ***** Executing S96localize-templates [ OK ] Executing S96ovf-data.pl [ OK ]
Executing S97compress-client-resources [ OK ] Executing S97create_platinum_forms.pl [ OK ]
Executing S97install_cas [ OK ] Executing S97install_cloud_support.pl [ OK ] Executing
S97install_geolocation.pl [ OK ] Executing S97install_ssl_inspection.pl [ OK ] Executing
S97update_modprobe.pl [ OK ] Executing S98check-db-integrity.sh [ OK ] Executing S98htaccess-
init [ OK ] Executing S98is-sru-finished.sh [ OK ] Executing S99correct_ipmi.pl [ OK ] Executing
S99start-system [ OK ] Executing S99z_db_restore [ OK ] Executing S99_z_cc-integrity.sh [ OK ]
Firstboot scripts finished. Configuring NTP... [ OK ] fatattr: can't open
'/mnt/disk0/.private2': No such file or directory fatattr: can't open '/mnt/disk0/.ngfw': No
such file or directory Model reconfigure detected, executing scripts Pinging mysql Found mysql
is running Executing 45update-sensor.pl [ OK ] Executing 55recalculate_arc.pl [ OK ] Starting
xinetd: Sat Jan 14 12:07:35 UTC 2017 Starting MySQL... Pinging mysql Pinging mysql, try 1
Pinging mysql, try 2 Found mysql is running Running initializeObjects... Stopping MySQL...
Killing mysqld with pid 22354 Wait for mysqld to exit\c done Sat Jan 14 12:07:57 UTC 2017
Starting sfidf... [ OK ] Starting Cisco ASA5506-X Threat Defense, please wait...No PM running!
...started. ... output omitted ... firepower login: admin Password: < Admin123 You must accept
the EULA to continue. Press <ENTER> to display the EULA: END USER LICENSE AGREEMENT ... Please
enter 'YES' or press <ENTER> to AGREE to the EULA: System initialization in progress. Please
stand by. You must change the password for 'admin' to continue. Enter new password: Confirm new
password: You must configure the network to continue. You must configure at least one of IPv4 or
IPv6. Do you want to configure IPv4? (y/n) [y]: Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: Enter an IPv4 address for the
management interface [192.168.45.45]: 10.48.66.83 Enter an IPv4 netmask for the management
interface [255.255.255.0]: 255.255.255.128 Enter the IPv4 default gateway for the management
interface [192.168.45.1]: 10.48.66.1 Enter a fully qualified hostname for this system
[firepower]: FTD5506 Enter a comma-separated list of DNS servers or 'none' []: 192.168.0.1 Enter
a comma-separated list of search domains or 'none' []: If your networking information has
changed, you will need to reconnect. For HTTP Proxy configuration, run 'configure network http-
proxy' Manage the device locally? (yes/no) [yes]: no Configure firewall mode?
(routed/transparent) [routed]: Configuring firewall mode ... Update policy deployment
information - add device configuration - add network discovery - add system policy You can
register the sensor to a Firepower Management Center and use the Firepower Management Center to
manage it. Note that registering the sensor to a Firepower Management Center disables on-sensor
Firepower Services management capabilities. When registering the sensor to a Firepower
Management Center, a unique alphanumeric registration key is always required. In most cases, to
register a sensor to a Firepower Management Center, you must provide the hostname or the IP
address along with the registration key. 'configure manager add [hostname | ip address ]
[registration key ]' However, if the sensor and the Firepower Management Center are separated by
a NAT device, you must enter a unique NAT ID, along with the unique registration key. 'configure
manager add DONTRESOLVE [registration key ] [ NAT ID ]' Later, using the web interface on the
Firepower Management Center, you must use the same registration key and, if necessary, the same
NAT ID when you add this sensor to the Firepower Management Center.

```

## 6단계

FMC에 FTD를 등록합니다.

```
> configure manager add 10.62.148.50 cisco Manager successfully configured. Please make note of  
reg_key as this will be required while adding Device in FMC. > show managers Host : 10.62.148.50  
Registration Key : **** Registration : pending RPC Status :
```

FMC에서 **Devices(디바이스) > Device Management(디바이스 관리)**를 클릭하여 FTD 디바이스를 추가합니다.

FMC에 FTD를 추가한 후에는 다음을 수행해야 합니다.

- 인터페이스, 라우팅 등의 디바이스 설정을 재구성합니다.

- VPN, QoS 등의 정책을 재구성합니다.

- 액세스 제어 정책, NAT 및 플랫폼 설정 등 이전에 적용한 정책과 설정을 다시 적용합니다.

## 관련 문서

[설치 및 업그레이드 가이드](#)

[Cisco ASA 또는 Firepower Threat Defense 디바이스 이미지로 다시 설치](#)