在 Firepower 设备上安装和升级 FTD

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 网络图
- 任务1.FTD软件下载
- 任务2.验证FXOS-FTD兼容性
- 任务3.将FTD映像上传到Firepower设备
- 任务4.配置FTD管理和数据接口
- 任务5.创建和配置新的逻辑设备
- 任务6.将FTD注册到Firepower管理中心(FMC)
- 任务7.升级FTD
- 解决方案
- 确认

Firepower 2100

- 在FP2100上安装FTD
- FP2100上的FTD升级

验证

故障排除

相关信息

简介

本文档介绍如何在Firepower设备上安装、升级和注册Firepower威胁防御(FTD)软件。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行FXOS 2.0(1.37)的Cisco Firepower 4140安全设备

- 运行6.1.0.330的Firepower管理中心

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

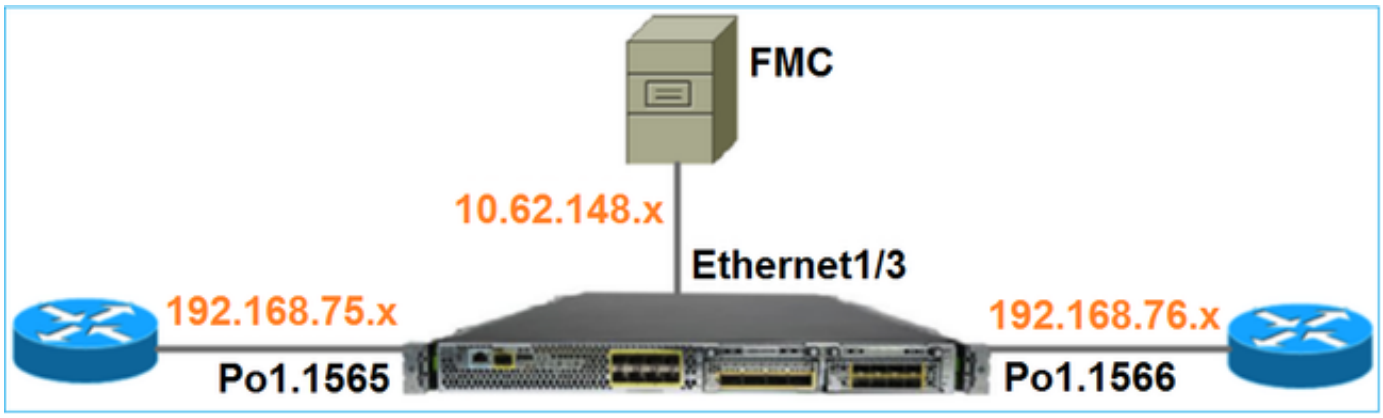
背景信息

FTD是可在以下平台上安装的统一软件映像：

- ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X、ASA5516-X
- ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X
- Firepower设备(FPR2100、FPR4100、FPR9300)
- VMware (ESXi)
- Amazon Web Services (AWS)
- 基于内核的虚拟机(KVM)
- 集成多业务路由器(ISR)模块

配置

网络图



任务1.FTD软件下载

导航到下一代防火墙(NGFW) > FirePOWER 4100系列> FirePOWER 4140安全设备，然后选择Firepower威胁防御软件（如图所示）。

任务2.验证FXOS-FTD兼容性

任务要求

验证机箱上运行的FXOS版本是否与要在安全模块中安装的FTD版本兼容。

解决方案

步骤1:检查FXOS-FTD兼容性。

在将FTD映像安装到模块/刀片之前，请确保Firepower机箱运行兼容的FXOS软件。在《FXOS兼容性指南》中，检查逻辑设备兼容性表。运行FTD 6.1.x所需的最低FXOS版本为1.1(4.95)，如表2所示：

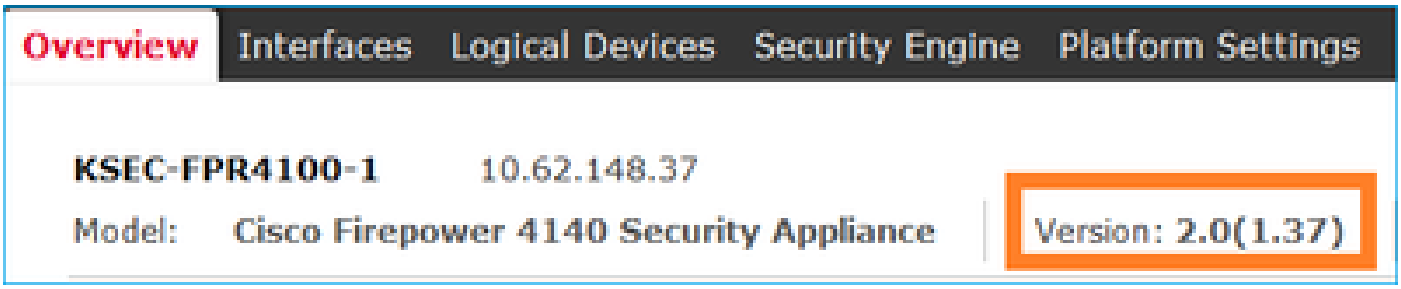
Table 2 Logical Device Compatibility

FXOS	ASA OS	Firepower Threat Defense
1.1(1.147)	9.4(1)	not supported
1.1(1.160)	9.4(1)	
...	...	
1.1(4.95)	9.6(1)	6.0.1.x
	9.6(2)	6.1

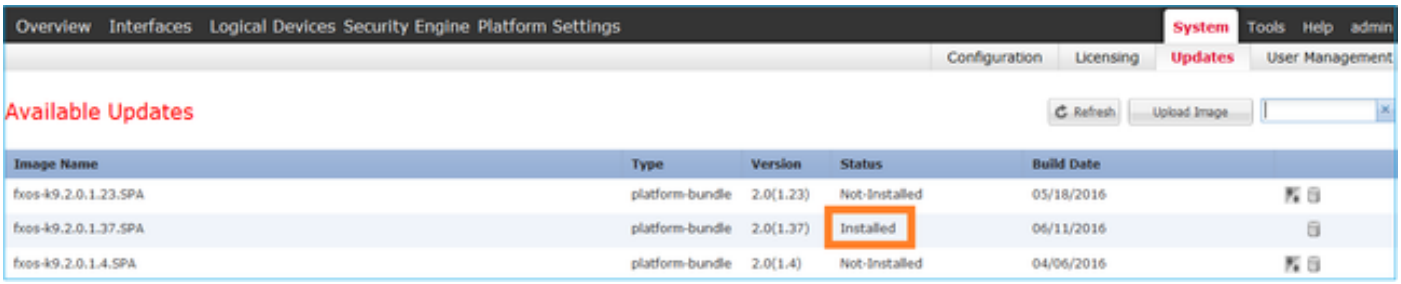
如果FXOS映像与目标FTD映像不兼容，请先升级FXOS软件。

验证FXOS映像

方法 1.从Firepower机箱管理器(FCM) UI概述页面，如图所示：



方法 2. 导航到FCM System > Update页，如图所示：



方法 3.从FXOS CLI：

<#root>

FPR4100#

show fabric-interconnect firmware

```
Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.01.35)
    Running-Sys-Vers: 5.0(3)N2(4.01.35)
```

Package-Vers: 2.0(1.37)

```
    Startup-Kern-Vers: 5.0(3)N2(4.01.35)
    Startup-Sys-Vers: 5.0(3)N2(4.01.35)
    Act-Kern-Status: Ready
    Act-Sys-Status: Ready
    Bootloader-Vers:
```

任务3.将FTD映像上传到Firepower设备

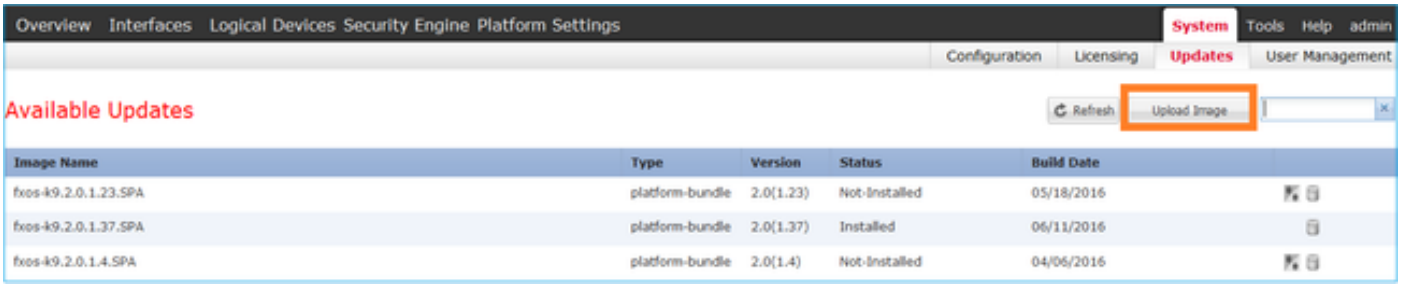
任务要求

将FTD映像上传到FPR4100机箱。

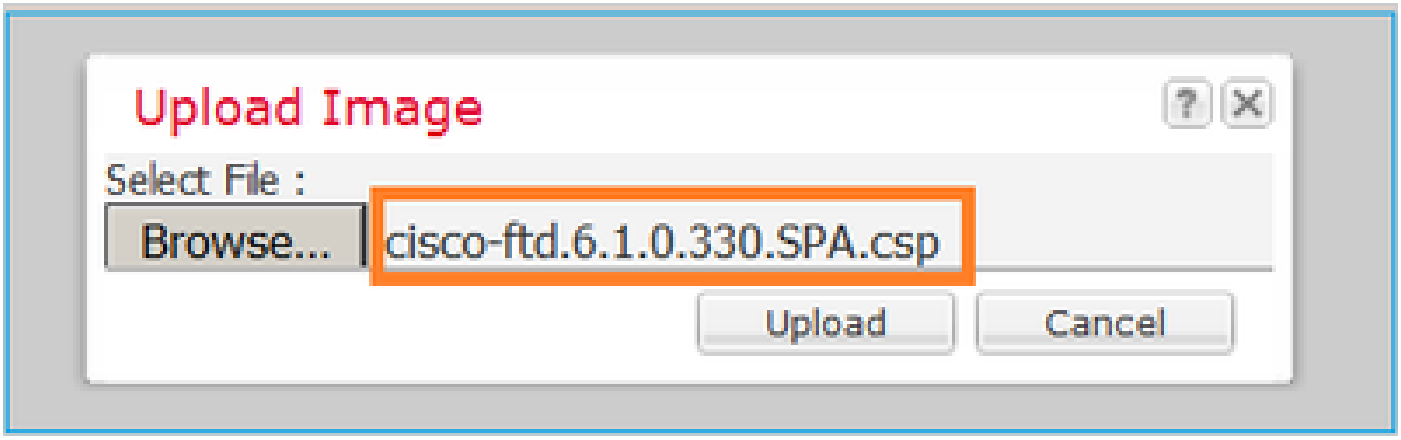
解决方案

方法1 -从FCM UI上传FTD映像。

登录FPR4100机箱管理器并导航到System > Updates选项卡。选择Upload Image上传文件，如图所示。

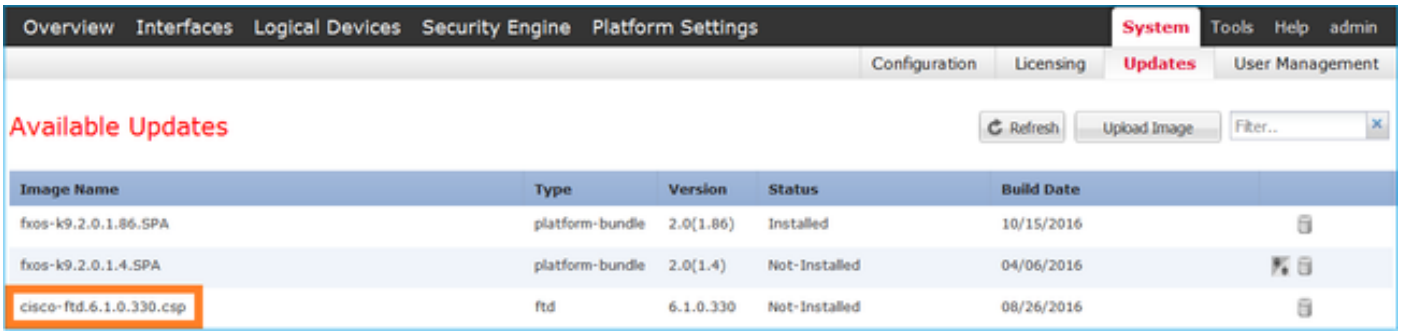


浏览并选择FTD映像文件，然后单击Upload，如图所示：



接受最终用户许可协议(EULA)。

验证如图所示。



方法2 -从FXOS CLI上传FTD映像

您可以从FTP、Secure Copy (SCP)、Secure FTP (SFTP)或TFTP服务器上传FTD映像。

在映像传输开始之前，验证机箱管理接口和远程服务器之间的连接：

```
<#root>

FPR4100#

connect local-mgmt

FPR4100(local-mgmt)#

ping 10.229.24.22

PING 10.229.24.22 (10.229.24.22) from 10.62.148.88 eth0: 56(84) bytes of data.
64 bytes from 10.229.24.22: icmp_seq=1 ttl=124 time=0.385 ms
64 bytes from 10.229.24.22: icmp_seq=2 ttl=124 time=0.577 ms
64 bytes from 10.229.24.22: icmp_seq=3 ttl=124 time=0.347 ms
```

要下载FTD镜像，请导航到此范围并使用download image命令：

```
<#root>

FPR4100#
```

```
scope ssa

FPR4100 /ssa #

scope app-software

FPR4100 /ssa/app-software #

download image ftp://ftp_username@10.229.24.22/cisco-ftd.6.1.0.330.SPA.csp

Password:
```

要监控映像上传进度，请执行以下操作：

```
<#root>

FPR4100 /ssa/app-software #

show download-task detail

Downloads for Application Software:

 File Name: cisco-ftd.6.1.0.330.SPA.csp

    Protocol: Ftp
    Server: 10.229.24.22
    Port: 0
    Userid: ftp
    Path:
    Downloaded Image Size (KB): 95040
    Time stamp: 2016-12-11T20:27:47.856

State: Downloading

Transfer Rate (KB/s): 47520.000000

    Current Task: downloading image cisco-ftd.6.1.0.330.SPA.csp from 10.229.24.22(FSM-STAGE:sam:dme:App
```

使用以下命令验证下载是否成功：

```
<#root>

FPR4100 /ssa/app-software #

show download-task

Downloads for Application Software:
    File Name                      Protocol   Server        Port       Userid    State
    ------------------------------ ---------- ------------- ---------- --------- -----
    cisco-ftd.6.1.0.330.SPA.csp    Ftp        10.229.24.22           0 ftp
```

Downloaded

有关其他详细信息：

<#root>

```
KSEC-FPR4100 /ssa/app-software #
```

show download-task fsm status expand

```
File Name: cisco-ftd.6.1.0.330.SPA.csp

    FSM Status:

        Affected Object: sys/app-catalogue/dnld-cisco-ftd.6.1.0.330.SPA.csp/fsm

Current FSM: Download

Status: Success

        Completion Time: 2016-12-11T20:28:12.889
        Progress (%): 100

        FSM Stage:

        Order  Stage Name                                Status       Try
        ------ ----------------------------------------- ------------ ---
        1      DownloadLocal
```

Success

```
 1
        2      DownloadUnpackLocal
```

Success

```
 1
File Name: Cisco_FTD_SSP_Upgrade-6.1.0-330.sh
```

该图像显示在机箱存储库中：

<#root>

```
KSEC-FPR4100 /ssa/app-software # exit
KSEC-FPR4100 /ssa #
```

show app

```
Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
```

```
    asa          9.6.2.3     N/A           cisco       Native       Application No

ftd          6.1.0.330
  N/A           cisco       Native       Application No
```

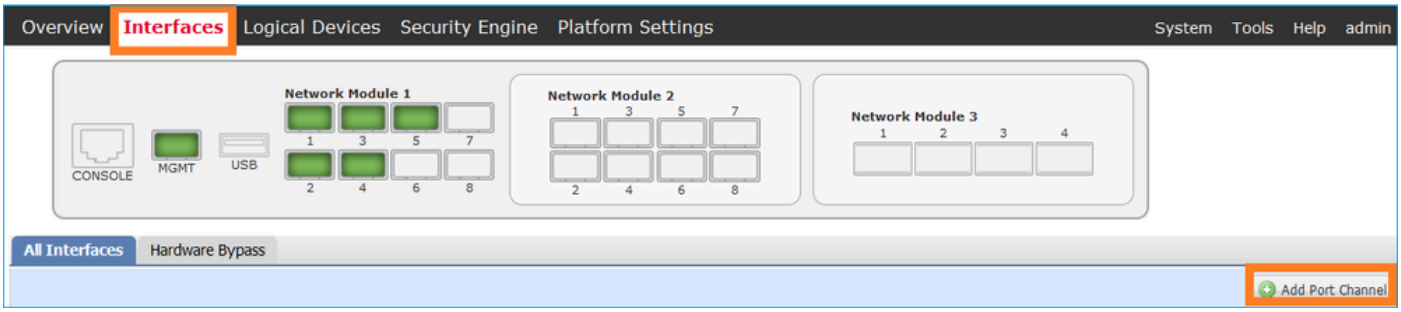
任务4.配置FTD管理和数据接口

任务要求

在Firepower设备上为FTD配置并启用管理和数据接口。

解决方案

要创建新接口，请登录FCM并导航到Interfaces 选项卡。查看当前接口。要创建新的端口信道接口，请选择Add Port Channel按钮，如图所示：



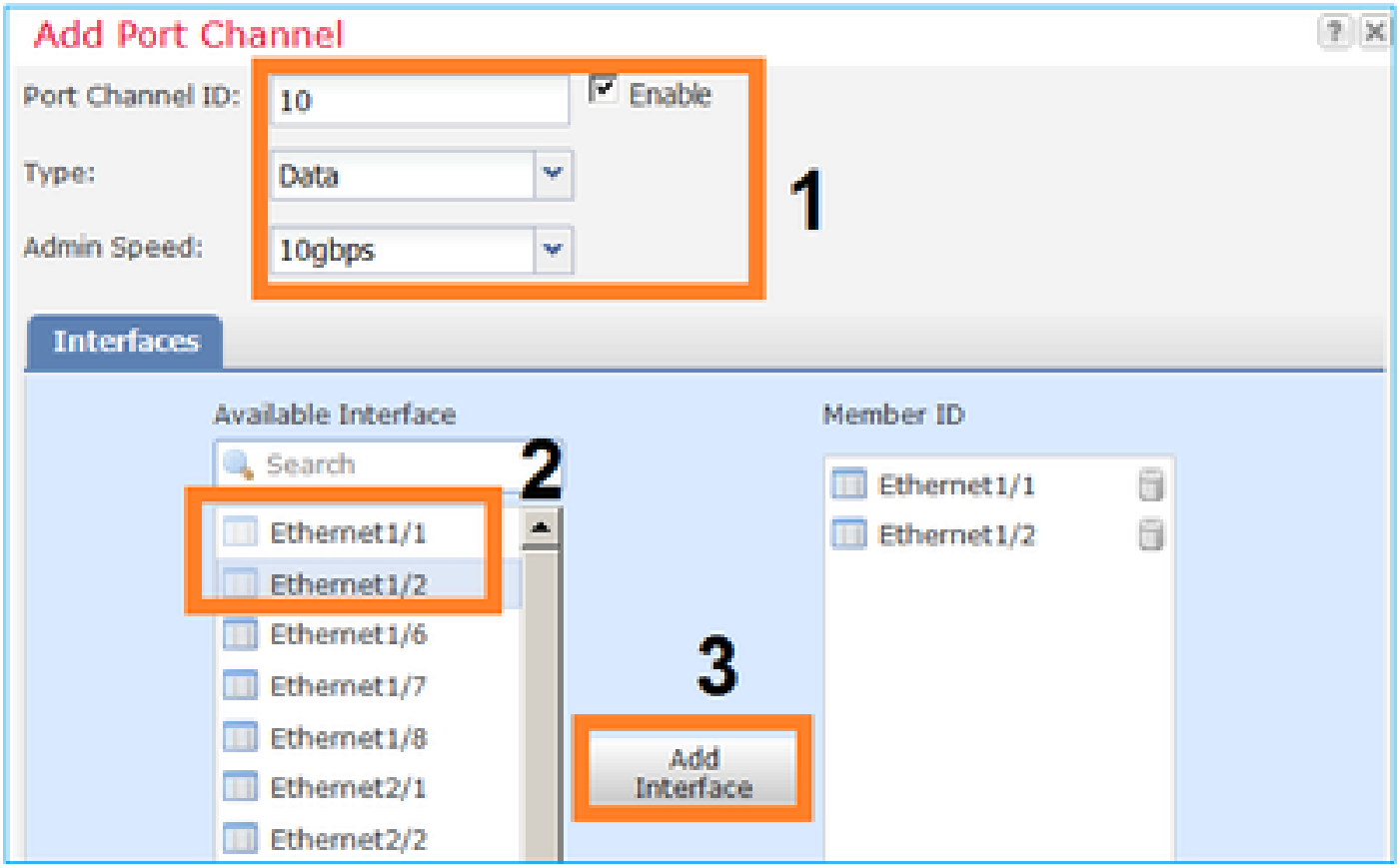
步骤1:创建端口通道数据接口。

创建新的端口通道接口，如图所示：

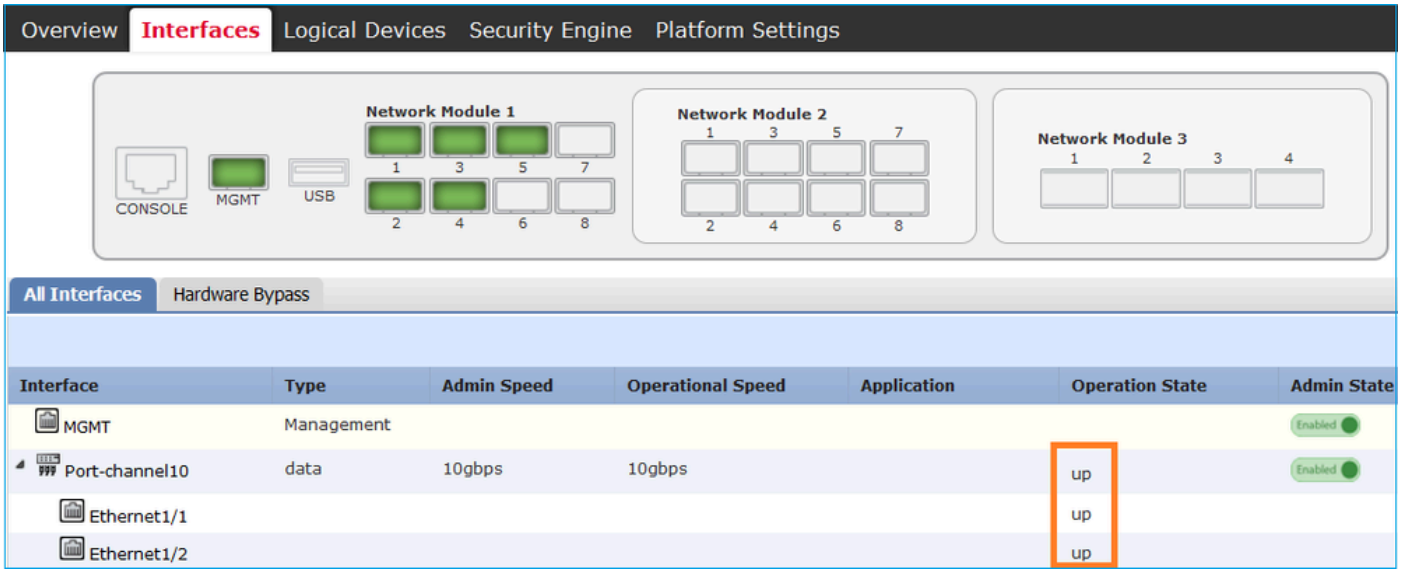
端口通道ID	10
类型	数据
enable	Yes
成员ID	Ethernet1/1、Ethernet 1/2

端口通道ID为1到47之间的值。

注意：PortChannel 48用于集群。

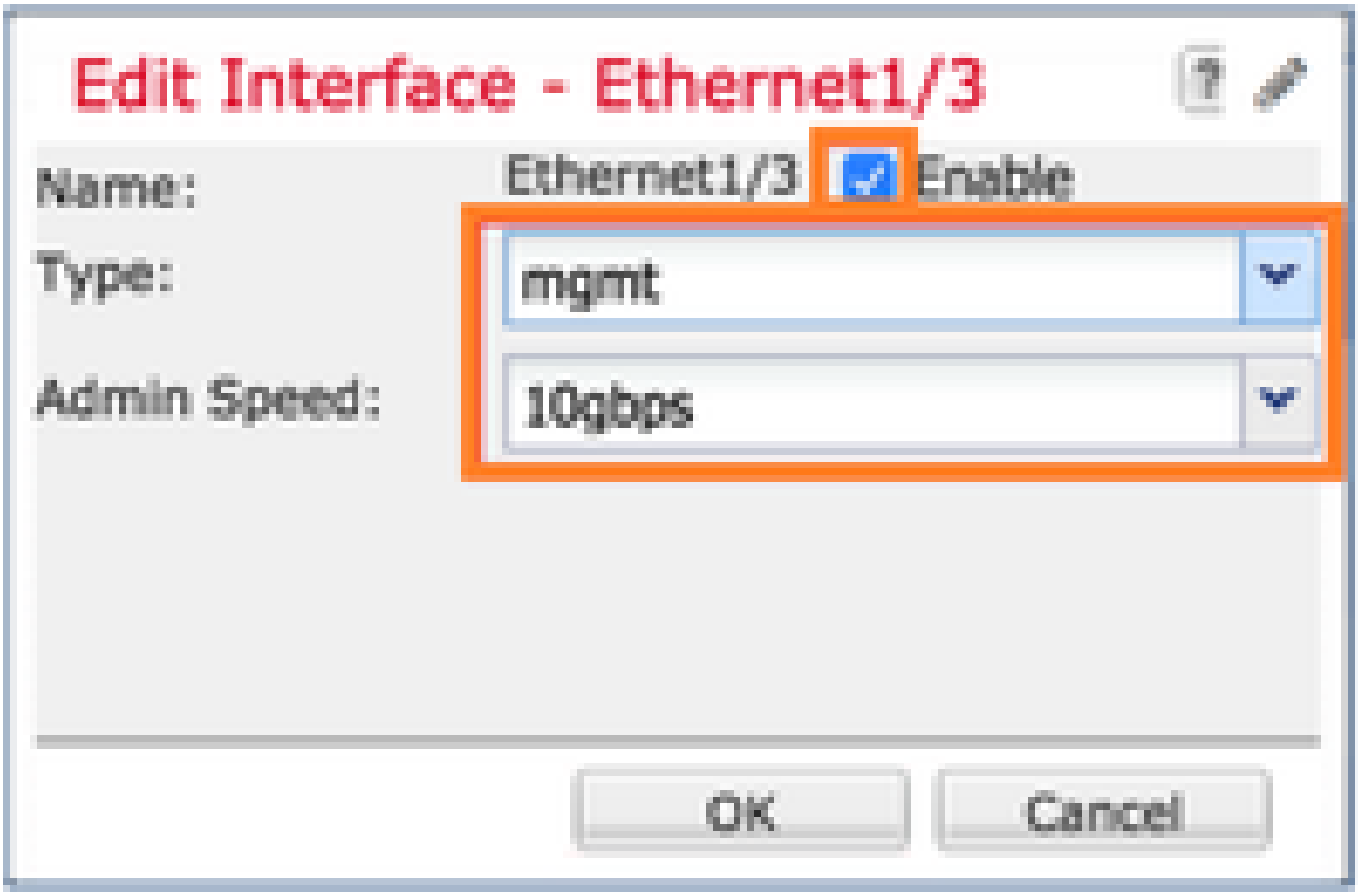


验证如图所示。



第二步：创建管理接口。

在Interfaces 选项卡上，选择接口，选择Edit，然后配置管理接口，如图所示：



任务5.创建和配置新的逻辑设备

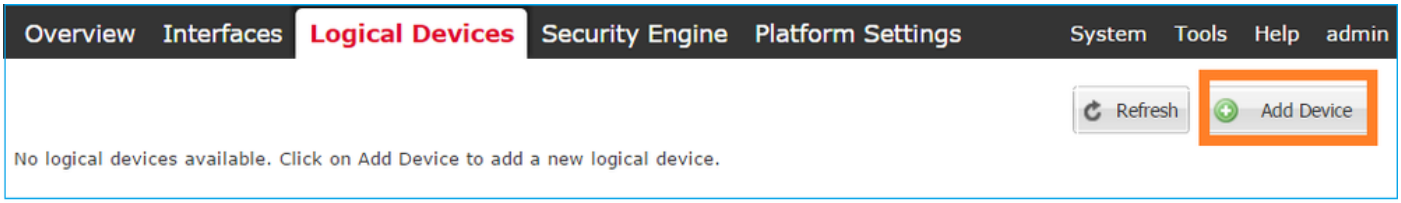
任务要求

创建FTD作为独立逻辑设备并进行部署。

解决方案

步骤1:添加逻辑设备。

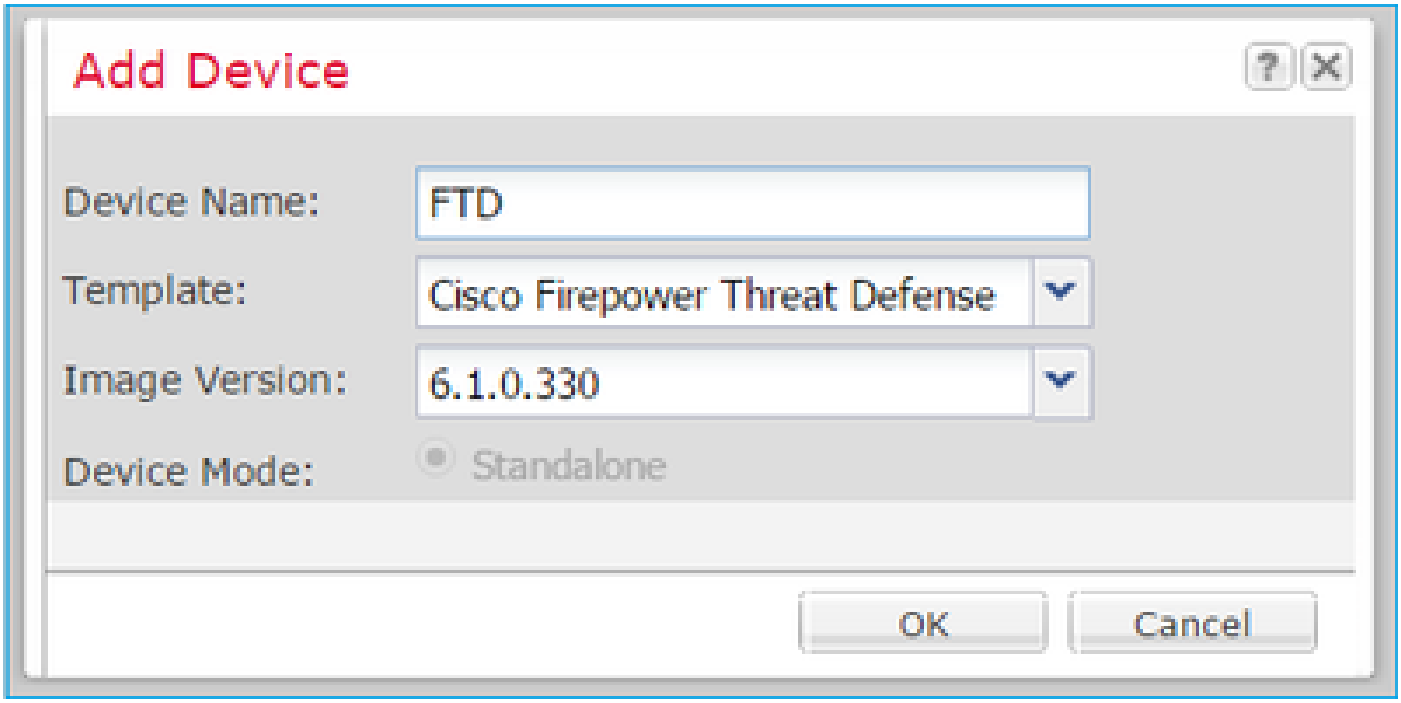
导航到逻辑设备选项卡并选择添加设备按钮以创建新的逻辑设备，如图所示：



使用图中所示的设置配置FTD设备：

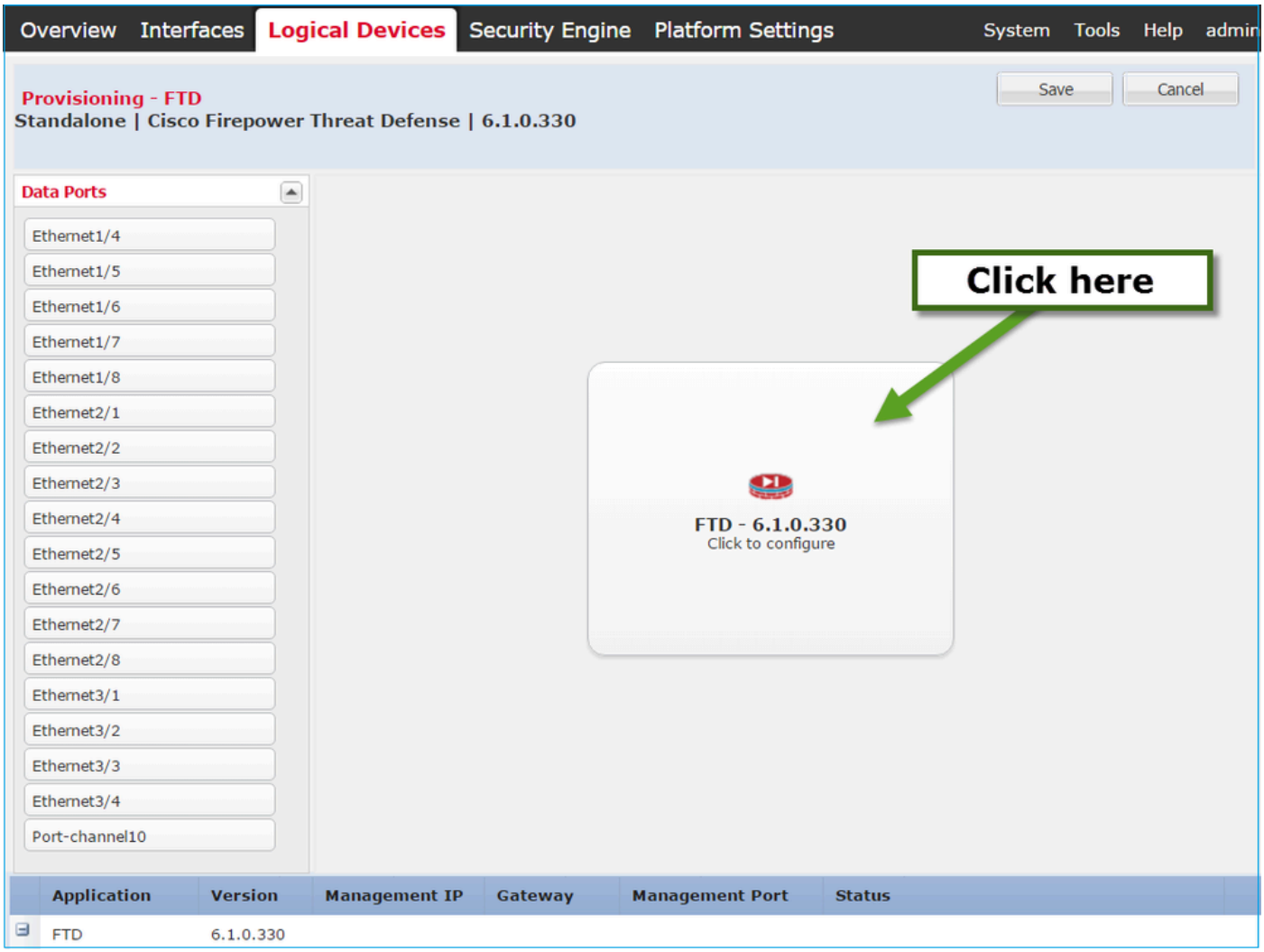
设备名	FTD
模板	Cisco Firepower威胁防御

映像版本	6.1.0.330



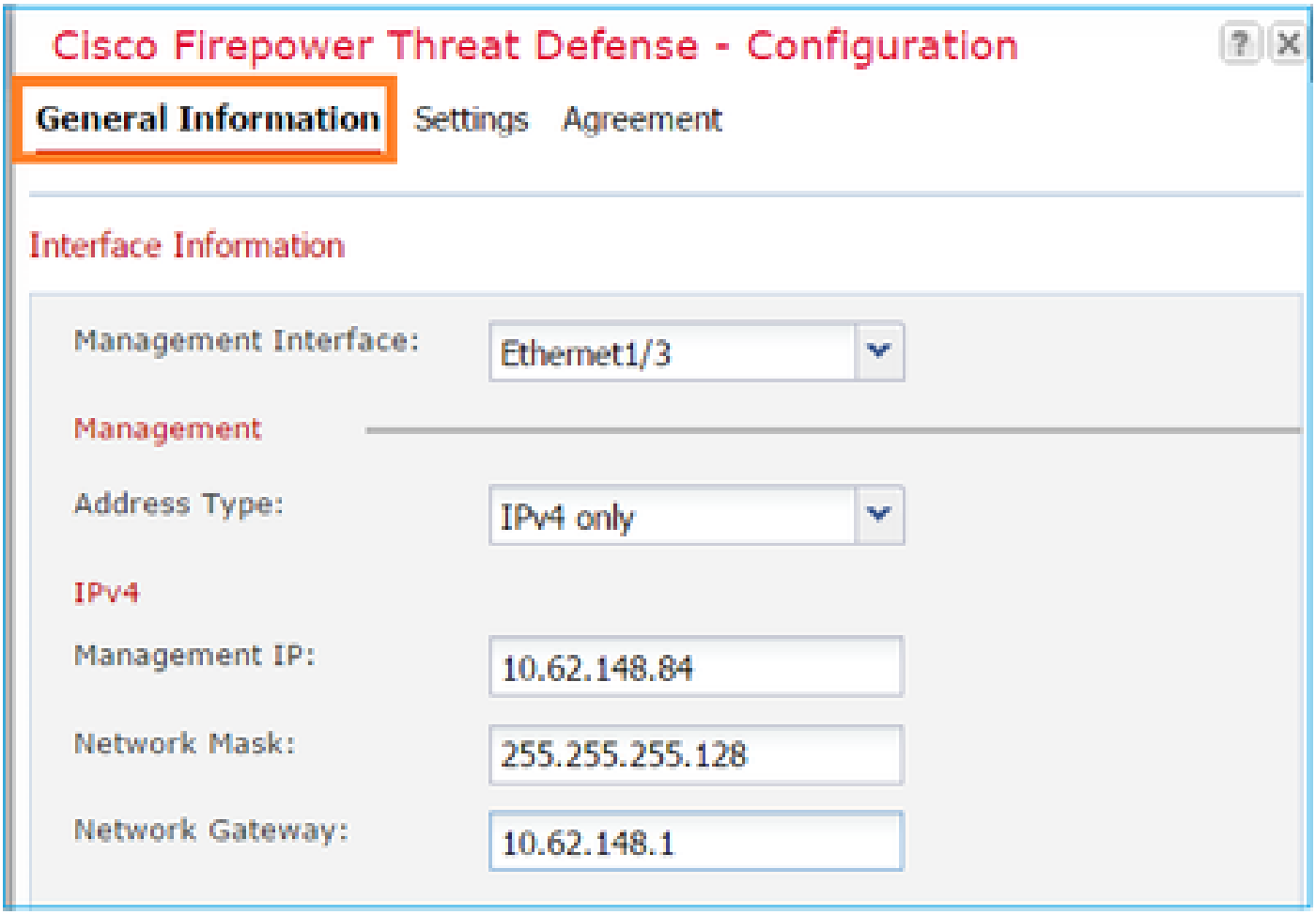
第二步：引导逻辑设备。

创建逻辑设备后，将显示Provisioning - device_name窗口。选择设备图标开始配置，如图所示：



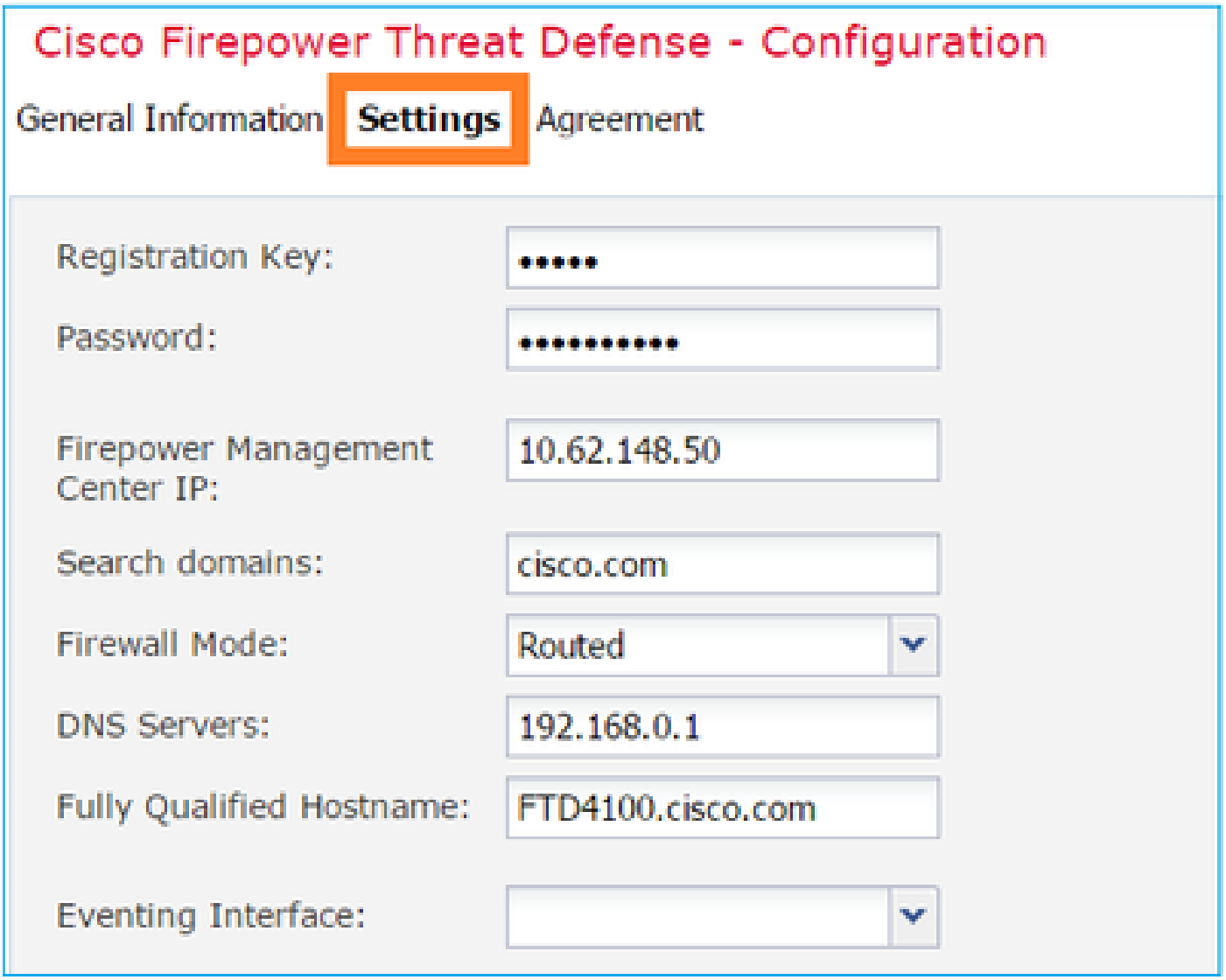
配置FTD常规信息选项卡，如图所示：

管理接口	Ethernet1/3
地址类型	仅IPv4
管理IP	10.62.148.84
网络掩码	255.255.255.128
网络网关	10.62.148.1



配置FTD Settings选项卡，如图所示：

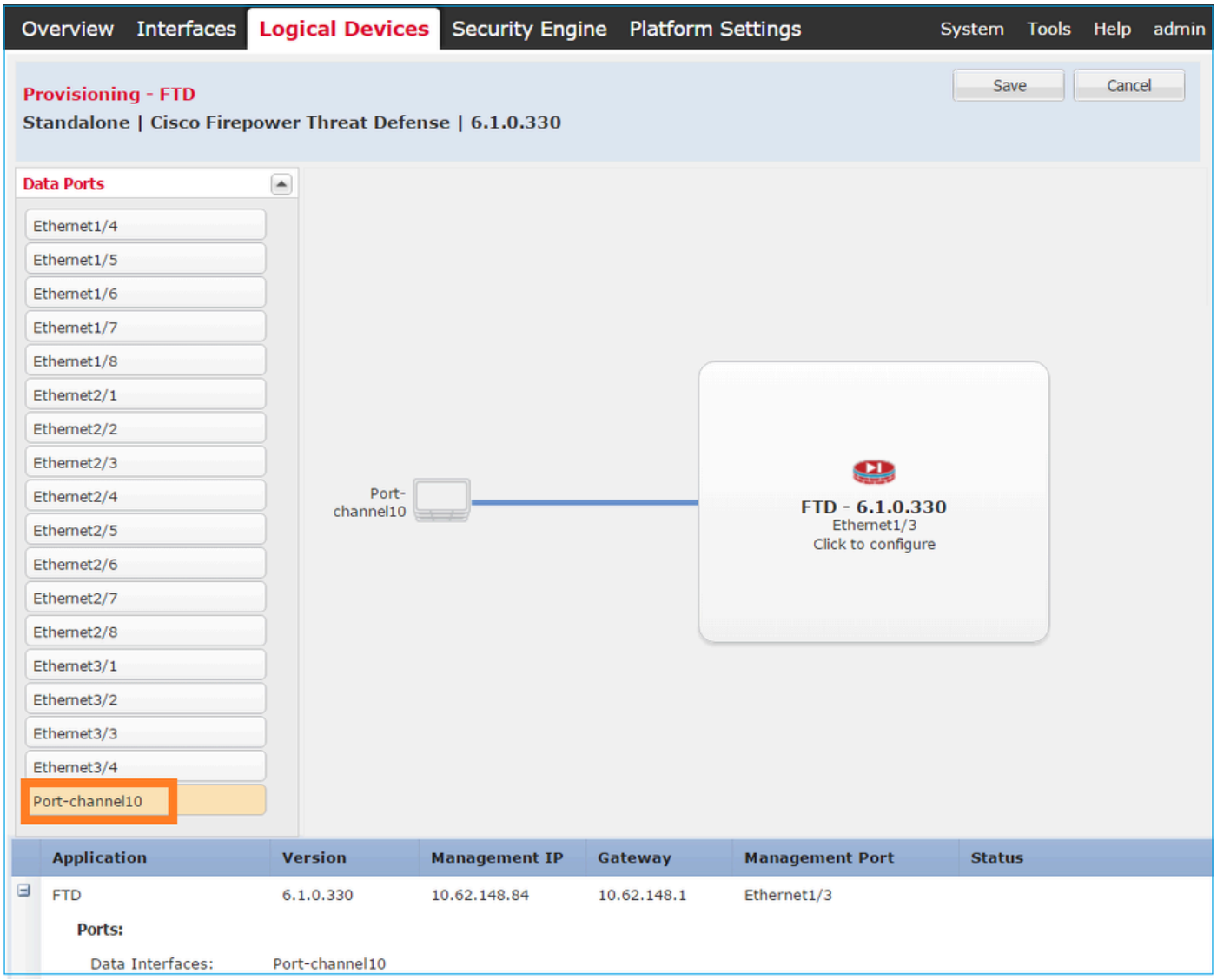
注册密钥	思科
密码	Pa$$w0rd
Firepower管理中心IP	10.62.148.50
搜索域	cisco.com
防火墙模式	路由
DNS Servers	192.168.0.1
完全限定的主机名	FTD4100.cisco.com
事件接口	-



确保接受协议，然后选择确定。

第三步：分配数据接口。

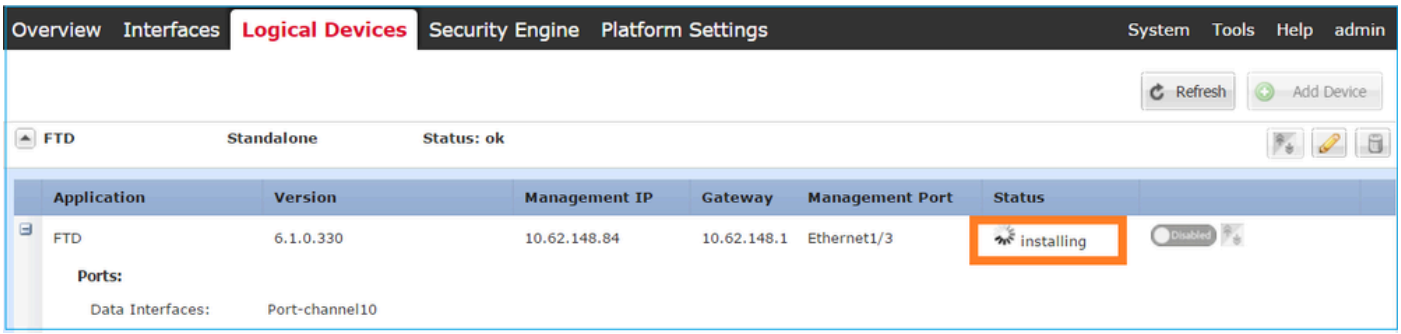
展开数据端口(Data Ports)区域并选择要分配给FTD的每个接口。在此场景中，分配了一个接口(Port-channel10)，如图所示：

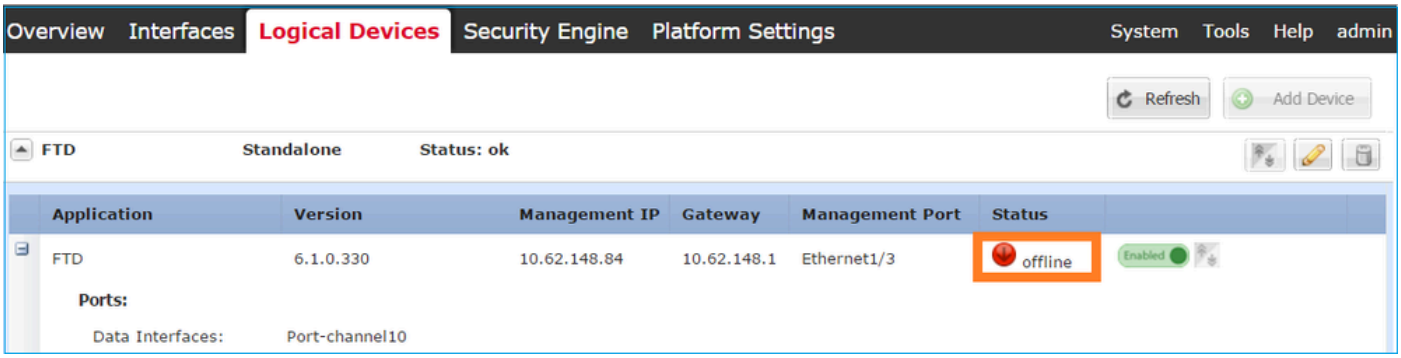


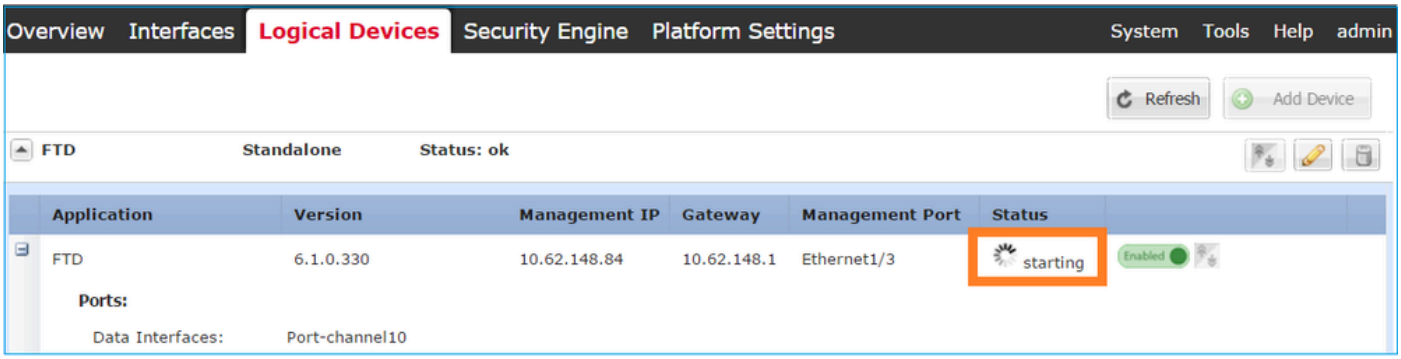
选择Save完成配置。

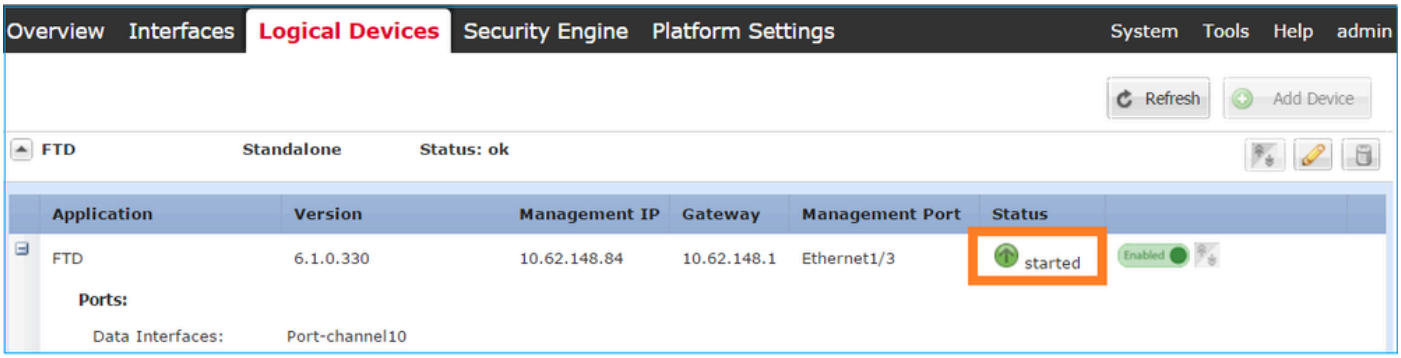
第四步：监控安装过程。

从FCM UI监控时，FTD安装过程如下（如图所示）：









从Firepower CLI监控安装过程：

<#root>

FPR4100#

connect module 1 console

```
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Cisco FTD: CMD=-start, CSP-ID=cisco-ftd.6.1.0.330__ftd_001_JAD19500F7YHCNL7715, FLAG=''
```

Cisco FTD starting ...

```
Registering to process manager ...
VNICs requested: 9,22
Cisco FTD started successfully.
Cisco FTD initializing ...
Firepower-module1>Setting up VNICs ...
```

```
Found Firepower management vnic  18.
No Firepower eventing vnic configured.
Updating /ngfw/etc/sf/arc.conf ...
Deleting previous CGroup Configuration ...

Initializing Threat Defense ...                                    [  OK  ]

Starting system log daemon...                                      [  OK  ]
Stopping mysql...
Dec 12 17:12:17 Firepower-module1 SF-IMS[14629]: [14629] pmtool:pmtool [ERROR] Unable to connect to UNI
Starting mysql...
Dec 12 17:12:17 Firepower-module1 SF-IMS[14641]: [14641] pmtool:pmtool [ERROR] Unable to connect to UNI
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 successed
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 successed
Starting nscd...
mkdir: created directory '/var/run/nscd'                           [  OK  ]
Starting , please wait......complete.
Firstboot detected, executing scripts
Executing S01virtual-machine-reconfigure                           [  OK  ]
Executing S02aws-pull-cfg                                          [  OK  ]
Executing S02configure_onbox                                       [  OK  ]
Executing S04fix-httpd.sh                                          [  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 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  ]
insmod: ERROR: could not insert module /lib/modules/kernel/drivers/uio/igb_uio.ko: File exists
rw console=ttyS0,38400 loglevel=2 auto kstack=128 reboot=force panic=1 ide_generic.probe_mask=0x1 ide1=
Fru Size                         : 512 bytes
Done
 VNIC command successful
 VNIC command successful
fatattr: FAT_IOCTL_GET_ATTRIBUTES: Inappropriate ioctl for device
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  ]
Mon Dec 12 17:16:15 UTC 2016
Starting MySQL...
Pinging mysql
```

```
Pinging mysql, try 1
Found mysql is running
Detecting expanded storage...
Running initializeObjects...
Stopping MySQL...
Killing mysqld with pid 32651
Wait for mysqld to exit\c
 done
Mon Dec 12 17:16:21 UTC 2016
Starting sfifd...                                                  [  OK  ]
Starting Cisco Firepower 4140 Threat Defense, please wait...No PM running!
...started.


Cisco FTD initialization finished successfully.

... output omitted ...


Reading from flash...
!
Cryptochecksum (changed): b1abfa7e 63faee14 affdddb0 9bc9d8cd

INFO: Power-On Self-Test in process.
.....................................................................
INFO: Power-On Self-Test complete.

INFO: Starting HW-DRBG health test (DRBG 0)...
INFO: HW-DRBG health test (DRBG 0) passed.
INFO: Starting HW-DRBG health test (DRBG 1)...
INFO: HW-DRBG health test (DRBG 1) passed.

INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.

Firepower-module1>
Firepower-module1>

show services status


Services currently running:
Feature | Instance ID | State | Up Since
-------------------------------------------------------------

ftd

 | 001_JAD19500F7YHCNL7715 |

RUNNING

 | :00:08:07
```

任务6.将FTD注册到Firepower管理中心(FMC)

任务要求

在FMC中注册FTD。

解决方案

步骤1:检验FTD和FMC之间的基本连接。

在向FMC注册FTD之前，请验证FTD和FMC之间的基本连接：

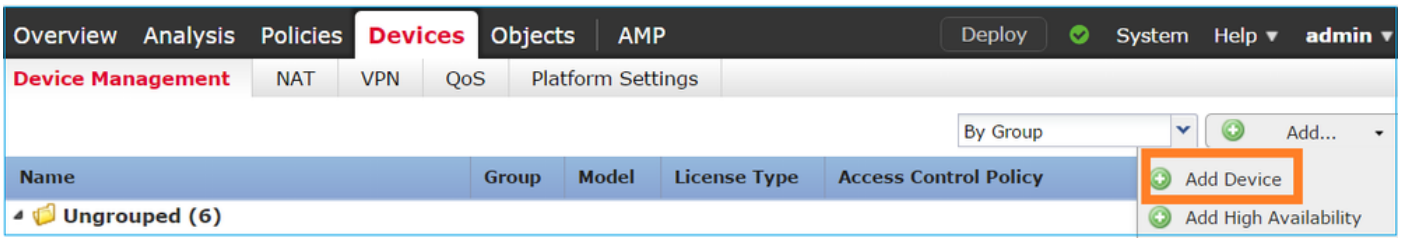
```
<#root>

Firepower-module1>

connect ftd


Connecting to ftd console... enter exit to return to bootCLI

>

ping system 10.62.148.50


PING 10.62.148.50 (10.62.148.50) 56(84) bytes of data.
64 bytes from 10.62.148.50: icmp_seq=1 ttl=64 time=0.133 ms
64 bytes from 10.62.148.50: icmp_seq=2 ttl=64 time=0.132 ms
64 bytes from 10.62.148.50: icmp_seq=3 ttl=64 time=0.123 ms
```

由于引导程序配置，FTD已配置管理器FMC：

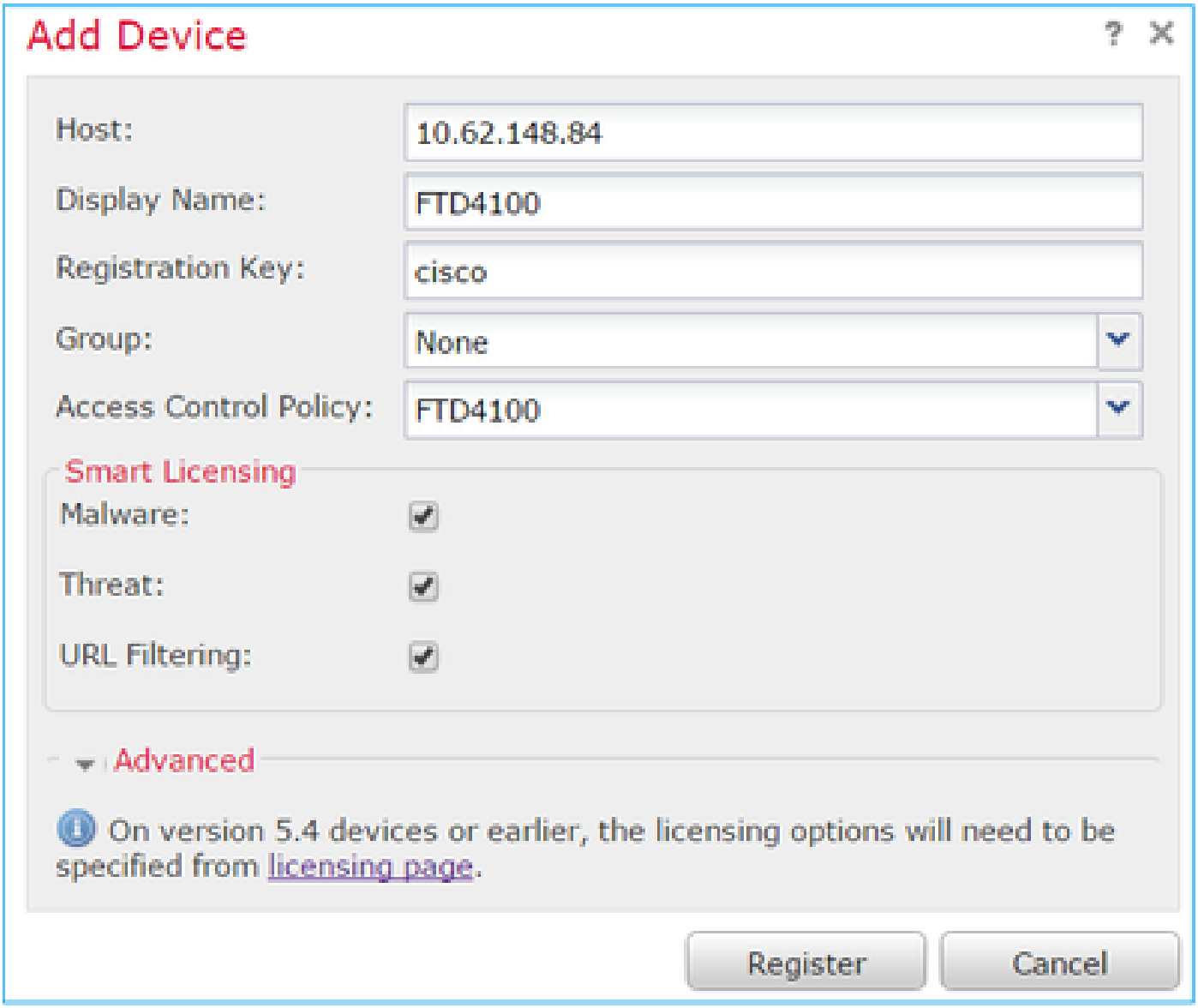
```
<#root>

>

show managers

Host                        : 10.62.148.50
Registration Key            : ****
Registration                :

pending

RPC Status                  :
```

第二步：将FTD添加到FMC。

在FMC上，导航到设备>设备管理选项卡，然后导航到添加..... > 添加设备，如图所示：



配置FTD设备设置，如图所示：

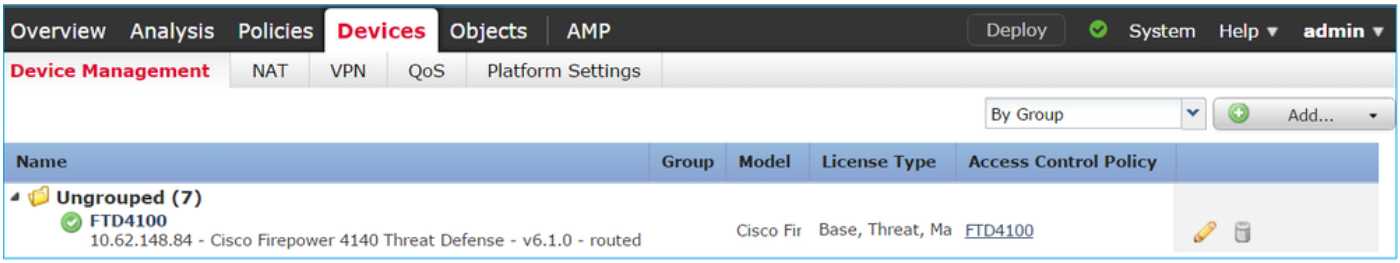


选择Register按钮。

在FMC上，检查Tasks（任务）以查看注册进度。除了注册之外，FMC还：

- 发现FTD设备（检索当前接口配置）。
- 部署初始策略。

成功注册如图所示：



注意：在版本6.1中，引入了Firepower设备管理器(FDM)以提供机上管理。Firepower设备上安装的FTD不能由FDM管理。

任务7.升级FTD

任务要求

将FTD从6.1.0.330升级到6.1.0.1。

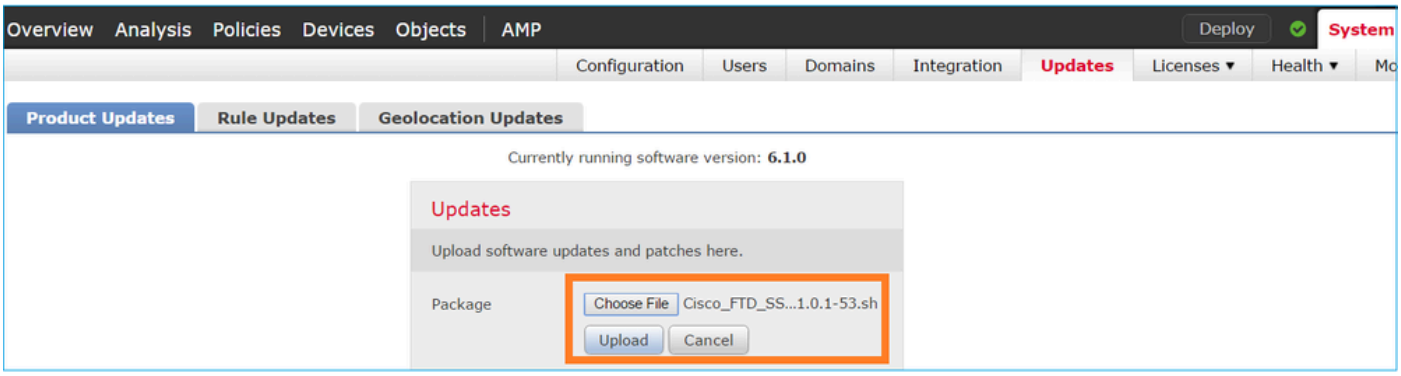
解决方案

步骤1:验证兼容性。

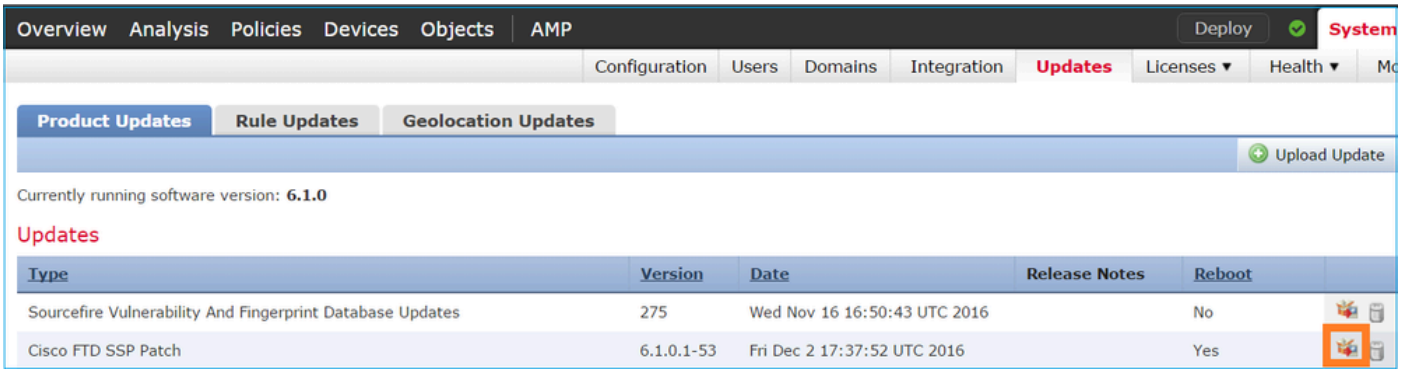
检查FXOS发行版本注释以确保目标FTD版本与FXOS软件兼容。如果需要，请先升级FXOS软件。

第二步：升级FTD。

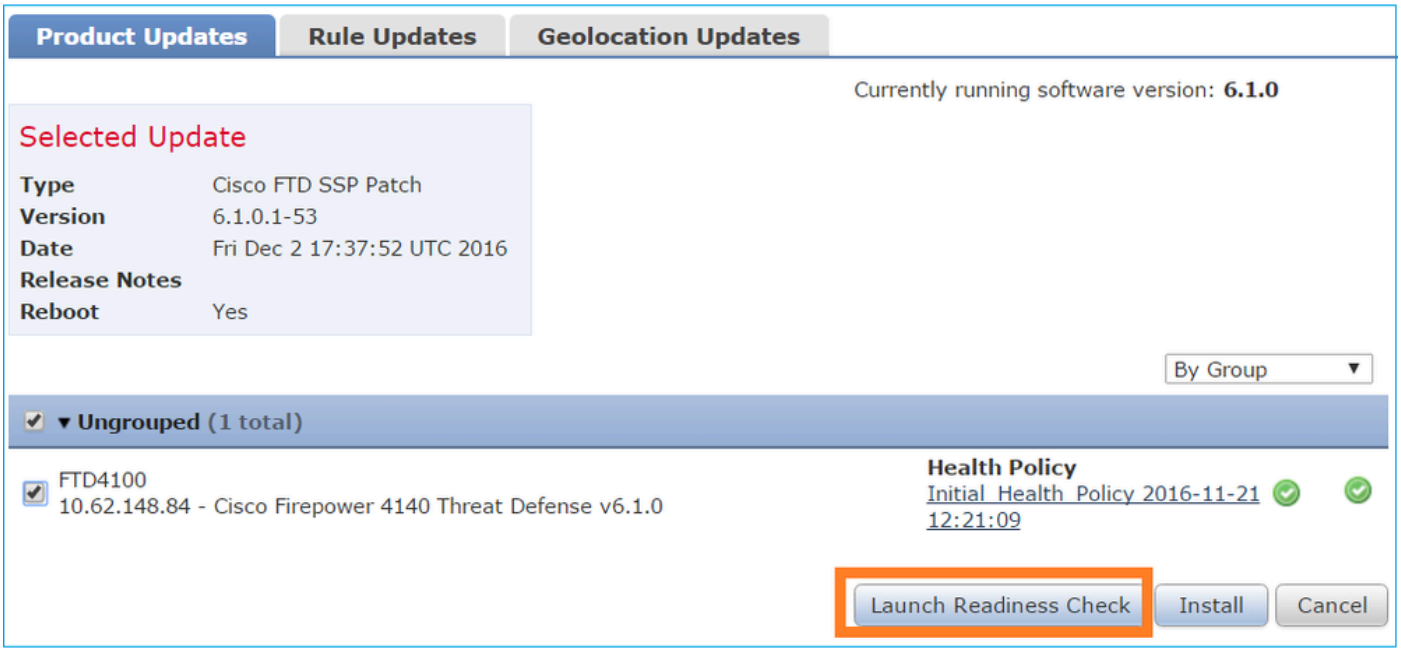
FTD软件由FMC而不是FCM管理。要升级FTD模块，请连接到FMC，导航到System > Updatespage，然后选择Upload Update，如图所示。



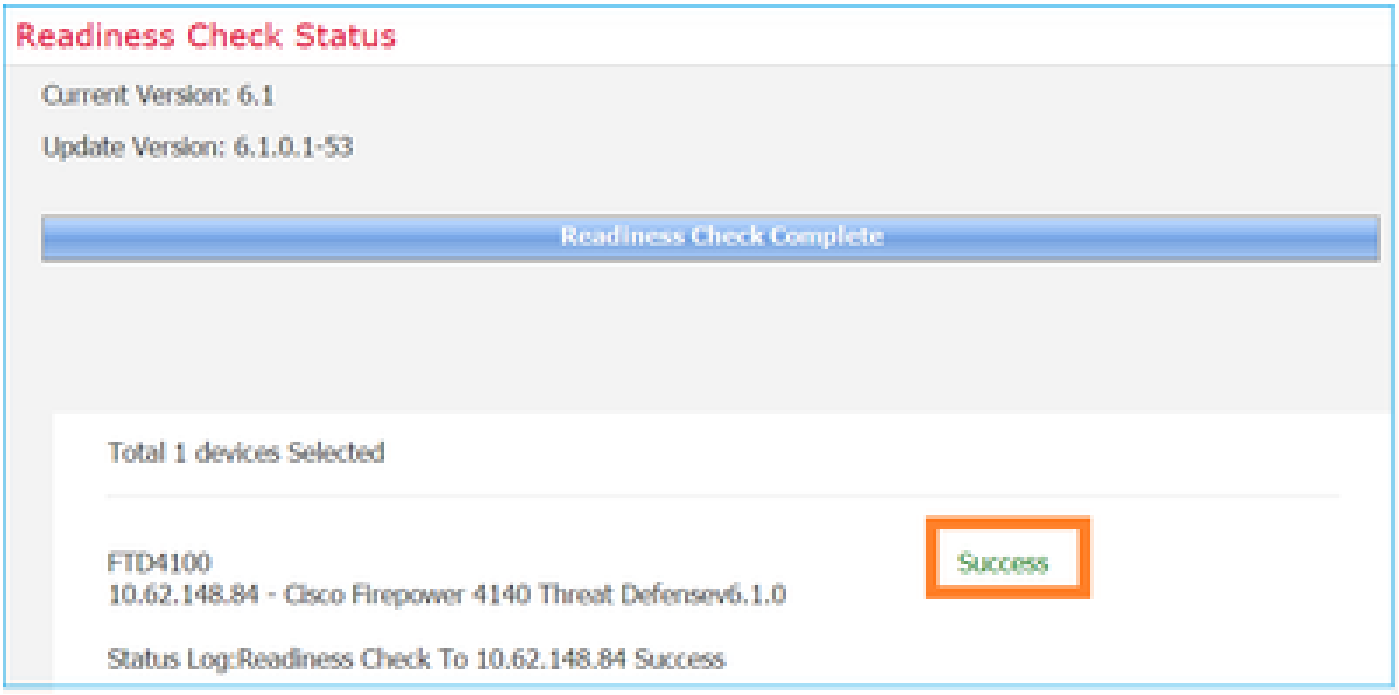
在FTD模块上安装更新，如图所示：



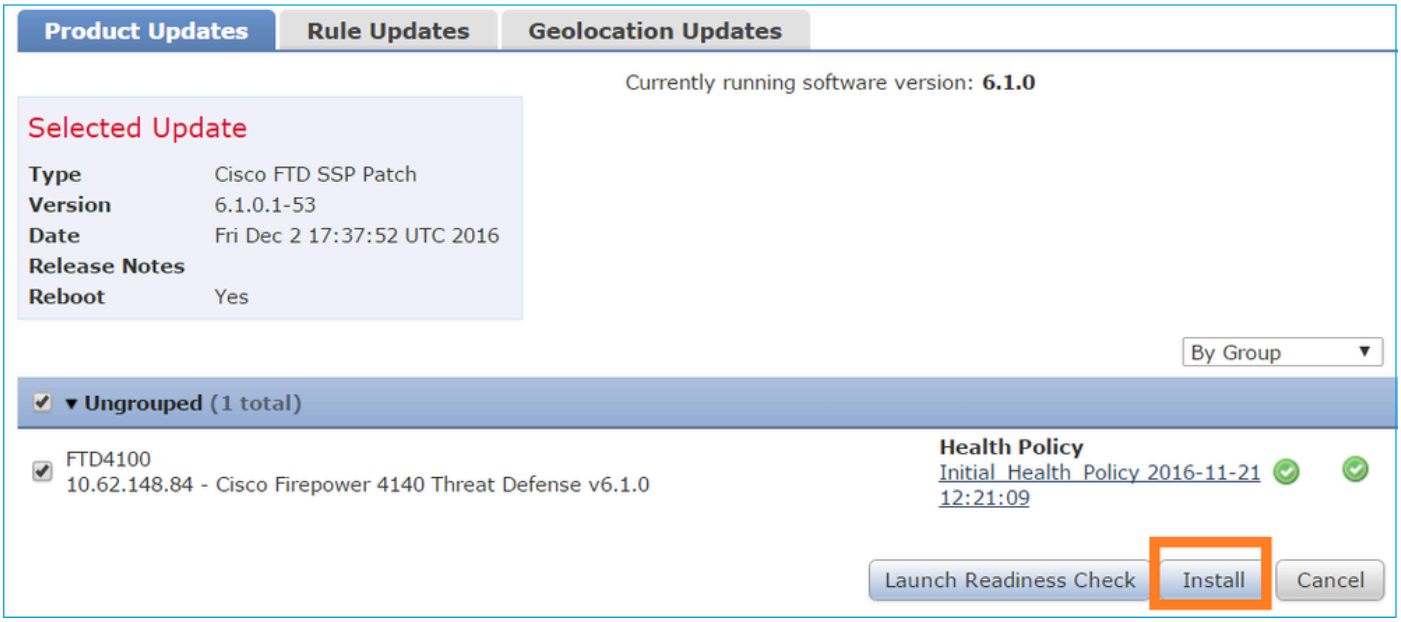
或者，您可以启动就绪性检查：



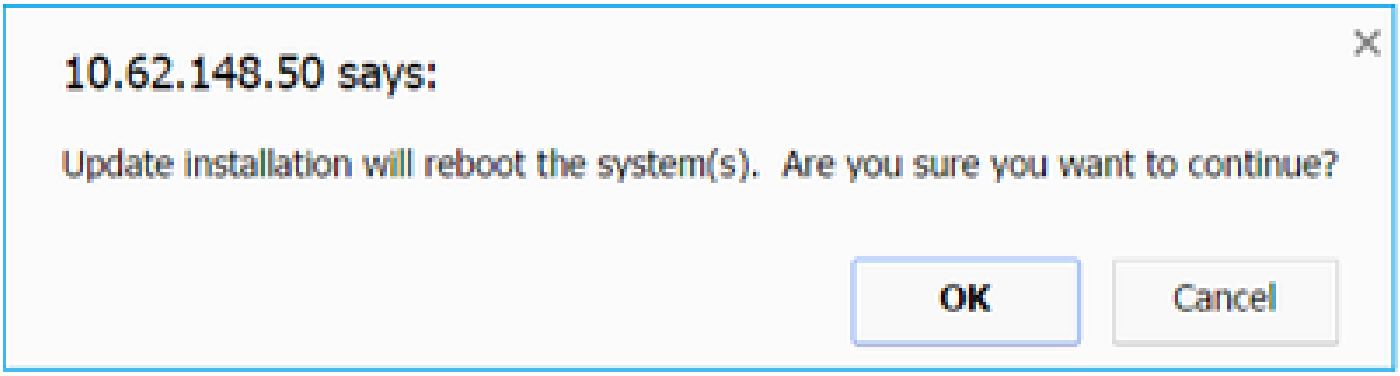
成功的就绪性检查如图所示：



要启动升级过程，请单击Install，如图所示：

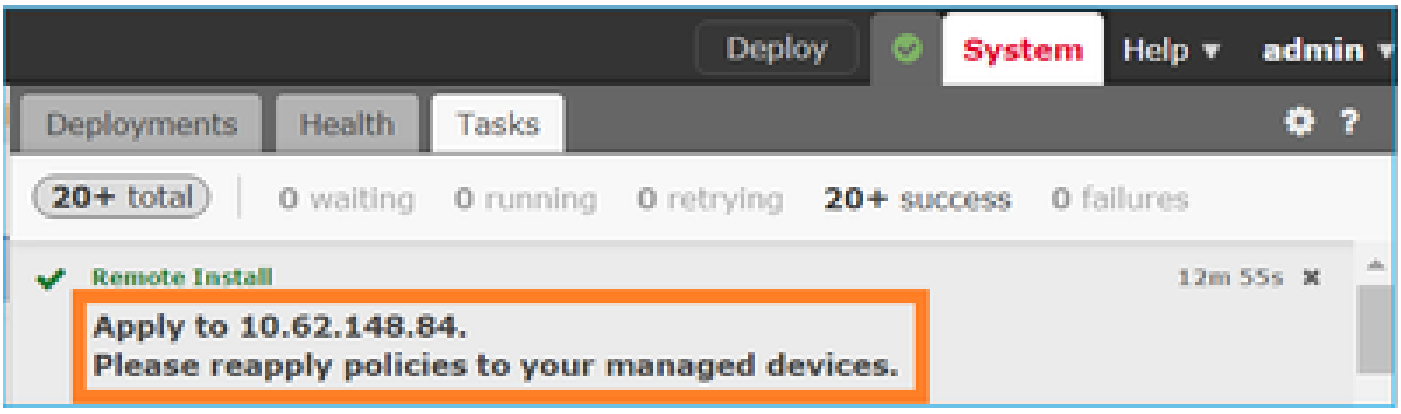


升级需要FTD重新启动，如图所示：



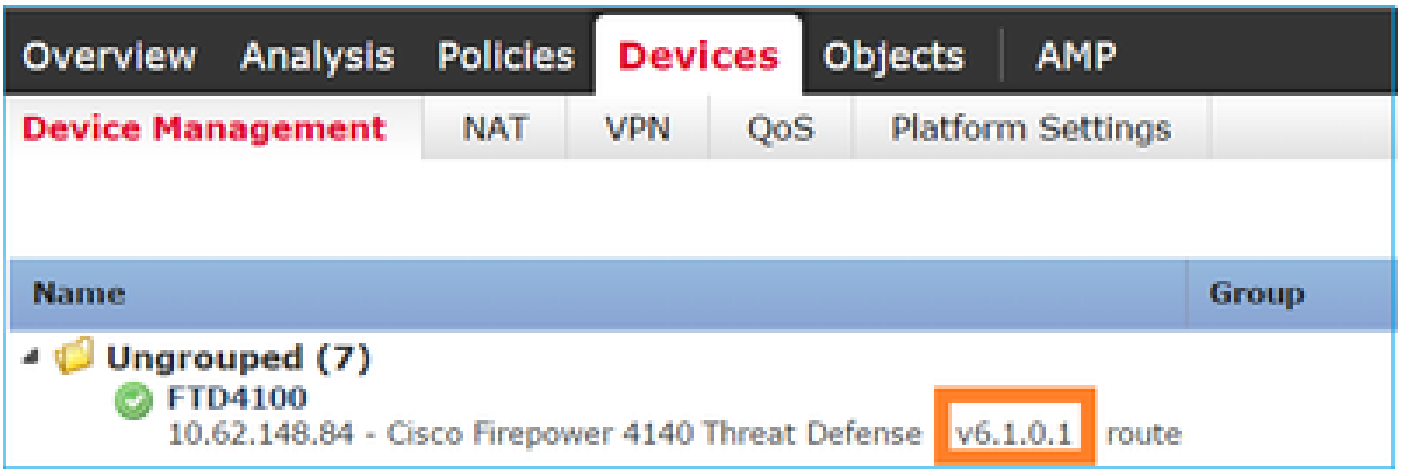
与FTD安装类似，可以从FMC UI (Tasks)监控FTD升级过程。可以从FTD CLI（CLISH模式）跟踪升级进度。

升级完成后，将策略部署到FTD，如图所示：

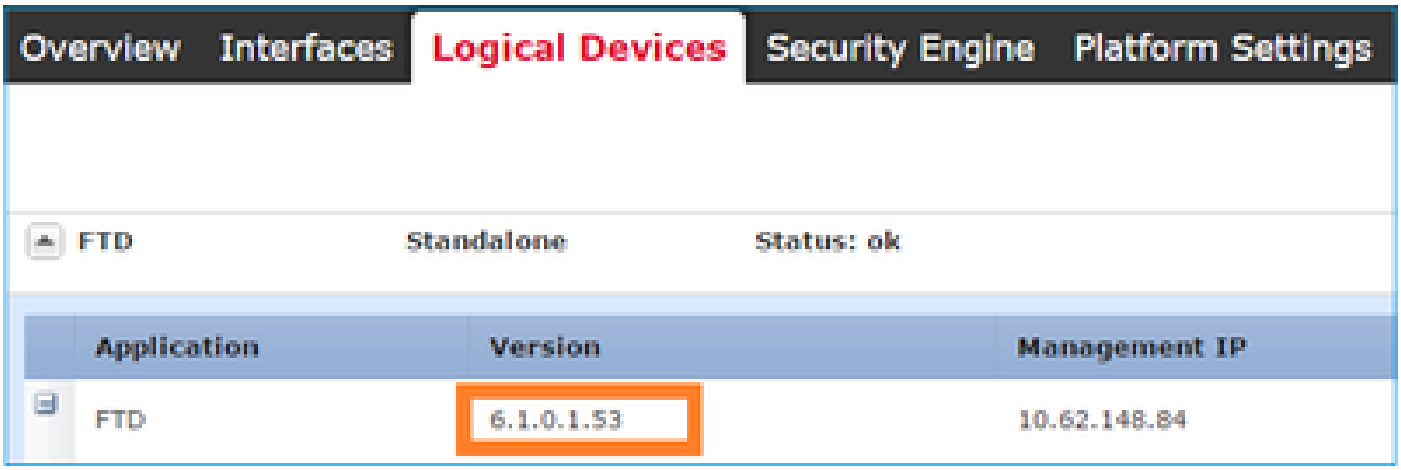


确认

从FMC UI中，如图所示：



从FCM UI中，如图所示：



从机箱CLI：

<#root>

FPR4100#

scope ssa

FPR4100 /ssa #

show app-instance

```
Application Name      Slot ID     Admin State      Operational State     Running Version Startup Version Cl
--------------------- ----------- ---------------- --------------------- --------------- --------------- --
ftd                   1           Enabled          Online
```

6.1.0.1.53

```
     6.1.0.330        Not Applicable
```

从FTD CLI：

<#root>

```
FPR4100#

connect module 1 console

Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

>

show version

---------------[ FTD4100.cisco.com ]----------------
Model                     : Cisco Firepower 4140 Threat Defense (76)

Version 6.1.0.1 (Build 53)

UUID                      : 22c66994-c08e-11e6-a210-931f3c6bbbea
Rules update version      : 2016-03-28-001-vrt
VDB version               : 275
------------------------------------------------------

>
```

Firepower 2100

Firepower 2100上的FTD使用包含FXOS和FTD映像的单个捆绑包。因此，安装和升级过程与FP4100/FP9300上的有所不同。

FP2100上的FTD安装

有4种不同的过程，具体取决于具体情况：

案例1：清除配置并使用相同的FTD映像重新启动系统。

案例2：使用新的应用软件版本重新映像系统。

案例3：将系统重新映像为其出厂默认设置。

案例4：将系统重新映像为其出厂默认设置（管理员密码恢复）。

有关每个案例及其程序的详细信息，请查看：

重新映像过程

案例2适用于大多数FTD安装案例，而案例3（格式化和从ROMMON引导）可用于特定案例（例如，系统不稳定或处于引导环路等）。

FP2100上的FTD升级

由于没有单独的FXOS套件，要升级FP2100上的FTD，请执行以下列出的步骤：

步骤1:验证兼容性。

如果FTD由FMC管理（机下管理），请检查软件目标FTD发行版本注释中的兼容性部分。

第二步：如有需要，请先升级FMC。始终运行等于或高于FTD目标软件版本的FMC软件版本。

第三步：升级FTD。

使用与FP4100/9300中记录的过程相同的过程。在FTD升级之前要阅读的重要文档：

- FTD发行版本注释（例如，如果要升级到版本6.3.0.2，请检查6.3.0.2发行版本注释以验证升级路径和所有相关详细信息。）版本说明
- FMC升级指南（章节：升级Firepower威胁防御：其他设备）Cisco Firepower管理中心升级指南，版本6.0-7.0

验证

当前没有可用于此配置的验证过程。

故障排除

当前没有故障排除此配置的特定可用资料。

相关信息

- FXOS兼容性指南
- Cisco Firepower NGFW文档
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。