升级安全防火墙的ASA主用/备用故障转移对

目录

简介

本文档介绍如何针对设备模式下的安全防火墙1000、2100和安全防火墙3100/4200的故障转移部署升级ASA。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全防火墙威胁防御。
- 思科自适应安全设备(ASA)配置。

使用的组件

本文档中的信息以下列软件版本为基础：

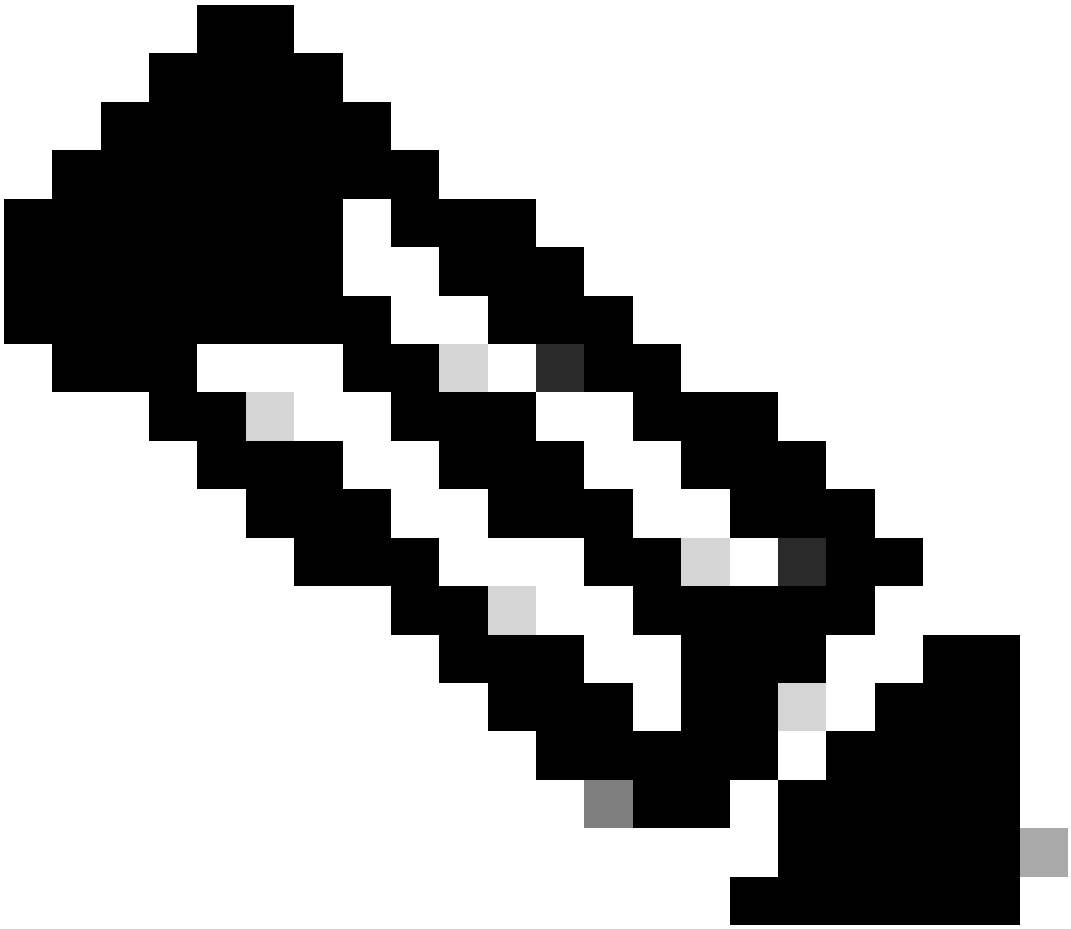
- Cisco 自适应安全设备软件版本 9.14(4)
- Cisco 自适应安全设备软件版本 9.16(4)

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。

配置

验证前提条件

步骤1:运行命令show fxos mode以验证设备是否处于装置模式



注意：对于版本9.13及更低版本的安全防火墙21XX，仅支持平台模式。在9.14版及更高版本中，设备模式是默认模式。

<#root>

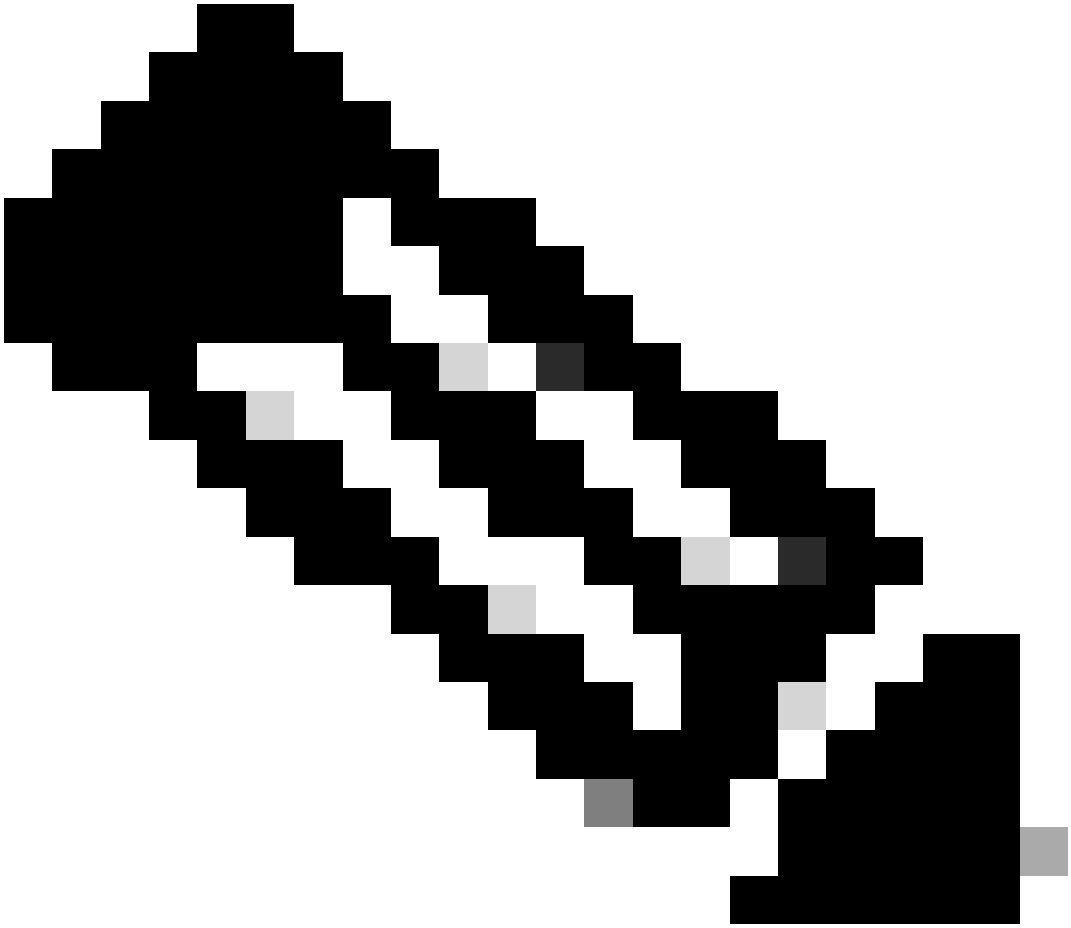
```
ciscoasa#

show fxos mode

Mode is currently set to appliance
```

第二步：验证兼容性。

请参阅思科安全防火墙ASA兼容性文档以验证FTD硬件平台和安全防火墙ASA软件之间的兼容性。请参阅

思科安全防火墙ASA兼容性

第三步：从Cisco软件中心下载升级软件包。



注意：对于安全防火墙1000/2100和安全防火墙3100/4200，无法分别安装ASA或FXOS；两个映像都是捆绑包的一部分。

请参阅链接的标题，了解捆绑包中的ASA和FXOS版本。请参阅安全防火墙1000/2100和3100/4200 ASA和FXOS捆绑包版本。

使用CLI升级

步骤1:重置ASDM映像。

在全局配置模式下连接到主设备并运行以下命令：

<#root>

ciscoasa(config)#

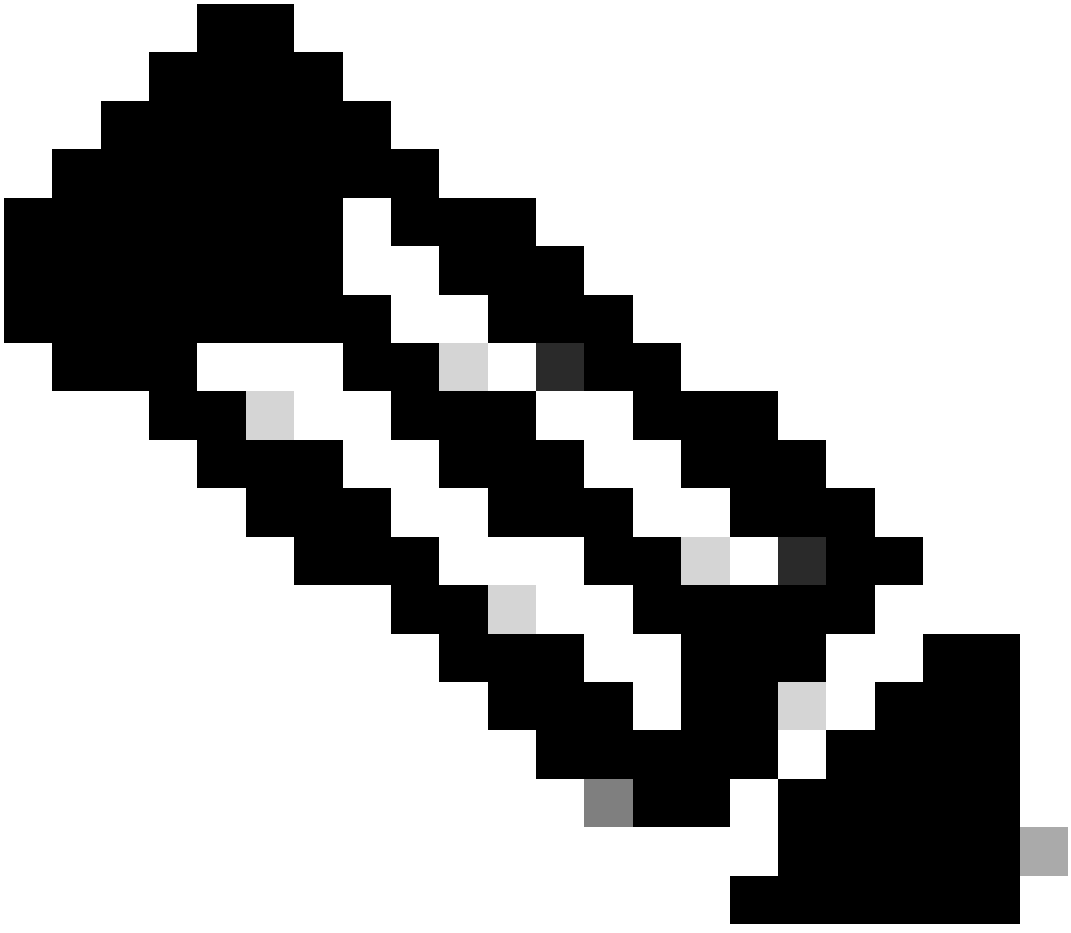
asdm image disk0:/asdm.bin

```
ciscoasa(config)# exit
ciscoasa#
```

copy running-config startup-config

```
Source filename [running-config]?
Cryptochecksum: 6beb01d1 b7a3c30f 5e8eb557 a8ebb8ca

12067 bytes copied in 3.780 secs (4022 bytes/sec)
```

第二步：将软件映像上传到主设备。



注意：在本文档中，您使用的是FTP服务器，但可以使用TFTP、HTTP或其他服务器类型。

<#root>

ciscoasa#

copy ftp://calo:calo@10.88.7.12/cisco-asa-fp2k.9.16.4.SPA disk0:/cisco-asa-fp2k.9.16.4.SPA

Address or name of remote host [10.88.7.12]?

Source username [calo]?

Source password []? **

Source filename [cisco-asa-fp2k.9.16.4.SPA]?

Destination filename [cisco-asa-fp2k.9.16.4.SPA]?

Accessing ftp:/calo:<password>@10.88.7.12/cisco-asa-fp2k.9.16.4.SPA...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Verifying file disk0:/cisco-asa-fp2k.9.16.4.SPA...

Writing file disk0:/cisco-asa-fp2k.9.16.4.SPA...

474475840 bytes copied in 843.230 secs (562842 bytes/sec)

第三步：将软件映像上传到辅助设备。

在主设备上运行命令。

<#root>

ciscoasa#

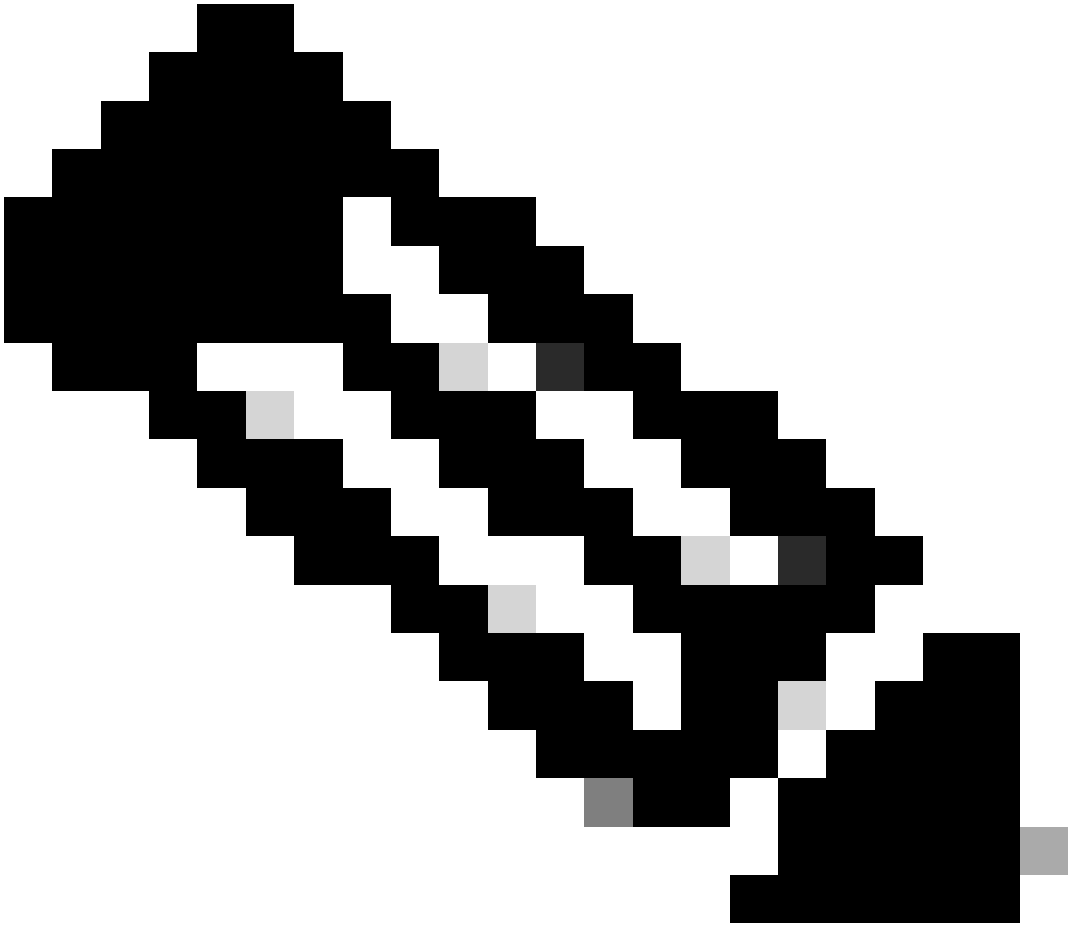
failover exec mate copy /noconfirm ftp://calo:calo@10.88.7.12/cisco-asa-fp2k.9.16.4.SPA disk0:/cisco-asa

Accessing ftp://calo :<password>@10.88.7.12/cisco-asa-fp2k.9.16.4.SPA...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Verifying file disk0:/cisco-asa-fp2k.9.16.4.SPA...

Writing file disk0:/cisco-asa-fp2k.9.16.4.SPA...

474475840 bytes copied in 843.230 secs (562842 bytes/sec)

第四步： 使用 **show running-config boot system** 命令检查您当前是否配置了引导映像。



注意：您可能尚未配置引导系统。

<#root>

ciscoasa(config)#

show running-config boot system

boot system disk0:/cisco-asa-fp2k.9.14.4.SPA

第 5 步（可选）： 如果已配置引导映像，则必须将其删除。

no boot system diskn：/asa_image_name

示例：

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp2k.9.14.4.SPA
```

第六步：选择要启动的映像。

```
<#root>

ciscoasa(config)#
```

boot system disk0:/cisco-asa-fp2k.9.16.4.SPA

```
The system is currently installed with security software package 9.14.4, which has:
   - The platform version:  2.8.1.172
   - The CSP (asa) version: 9.14.4
Preparing new image for install...
!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.16.4 will do the following:
   - upgrade to the new platform version 2.10.1.217
   - upgrade to the CSP ASA version 9.16.4
After installation is complete, ensure to do write memory and reload to save this config and apply the
Finalizing image install process...

Install_status: ready.............................
Install_status: validating-images....
Install_status: upgrading-npu
Install_status: upgrading-system.
Install_status: update-software-pack-completed
```

步骤 7.使用copy running-config startup-config命令保存配置。

步骤 8重新加载辅助设备以安装新版本。

```
<#root>

ciscoasa(config)#

failover reload-standby
```

等到辅助设备加载。

步骤 9备用设备重新加载后，将主设备从主用状态更改为备用状态。

```
<#root>

ciscoasa#

no failover active
```

步骤 10重新加载新的备用设备以安装新版本。您必须连接到新的主用设备。

```
<#root>
```

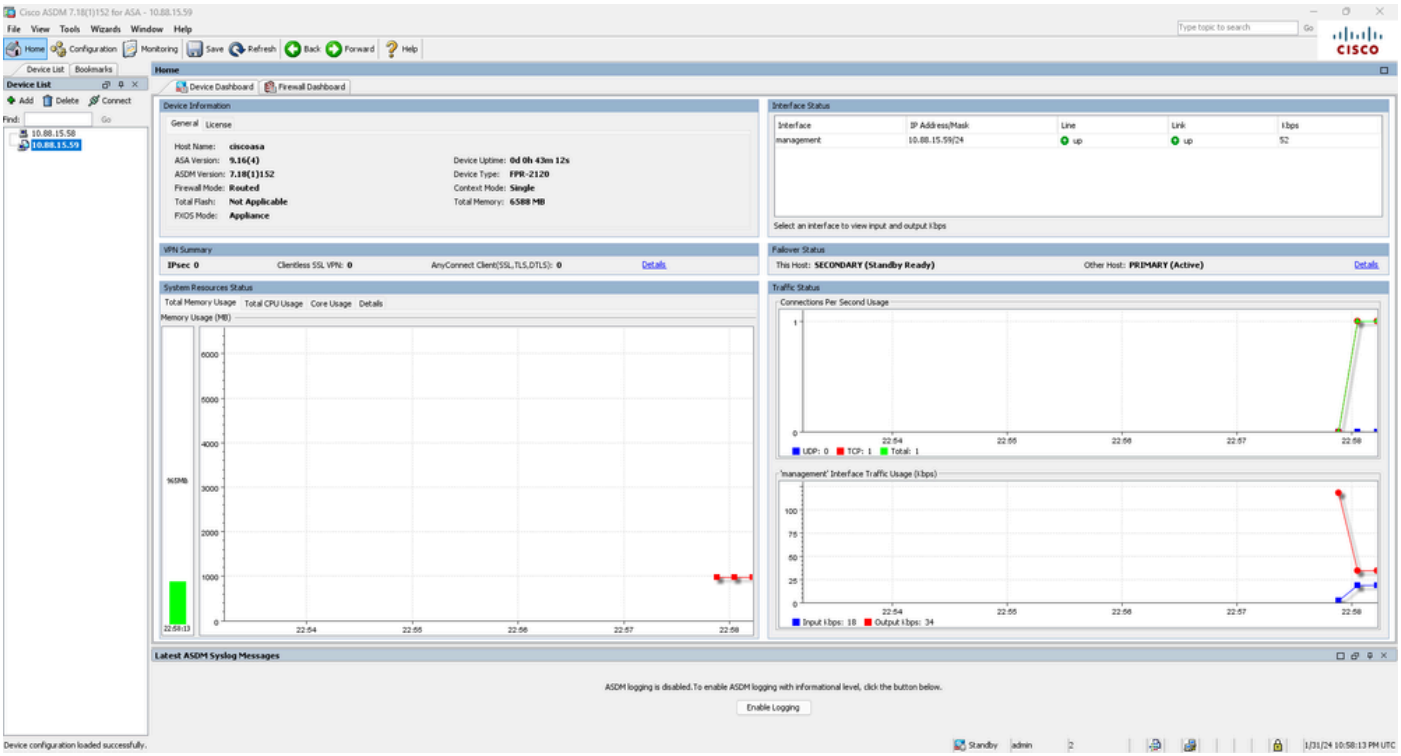
ciscoasa(config)#

```
failover reload-standby
```

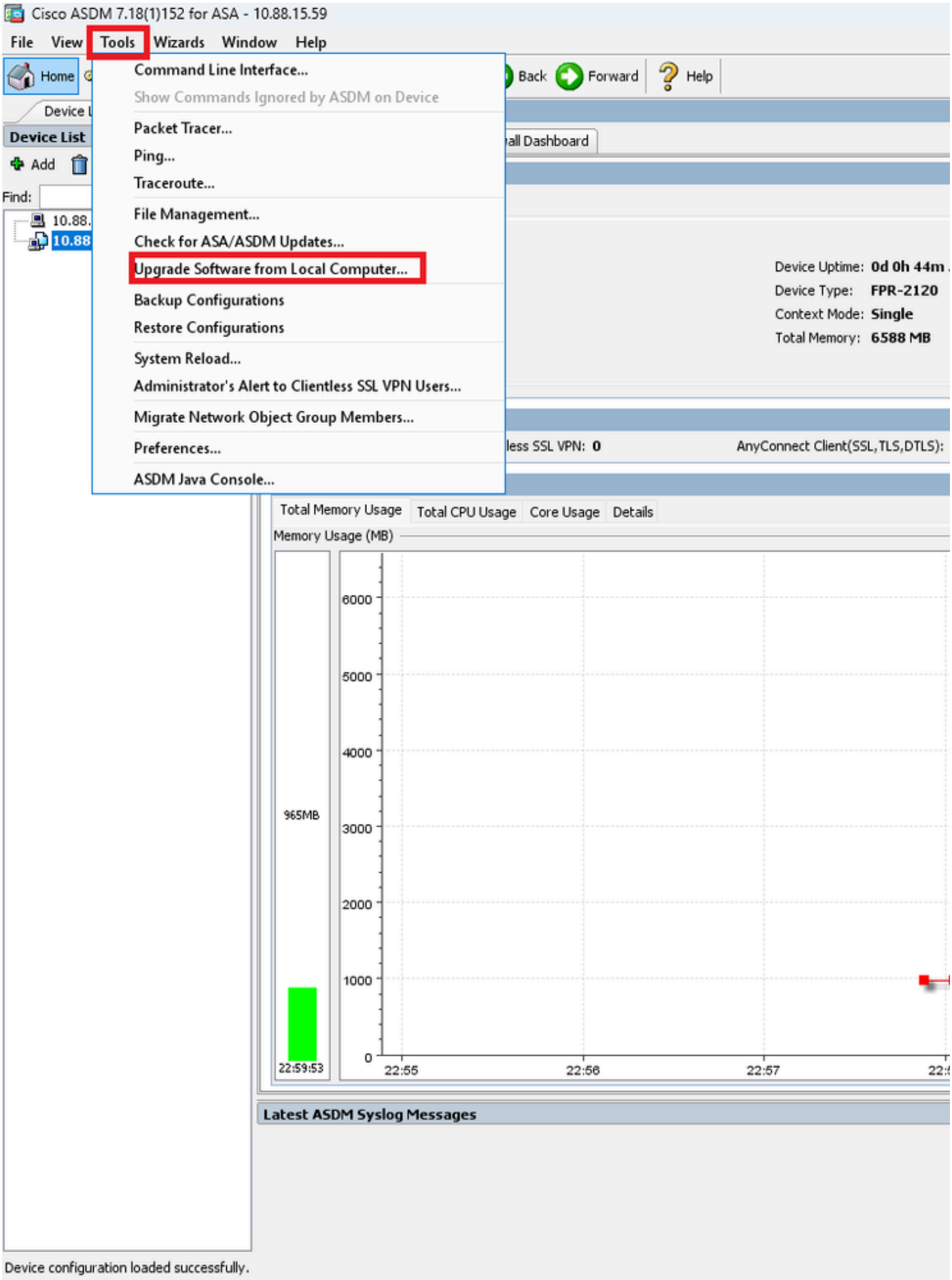
加载新的备用设备后，升级完成。

使用ASDM升级

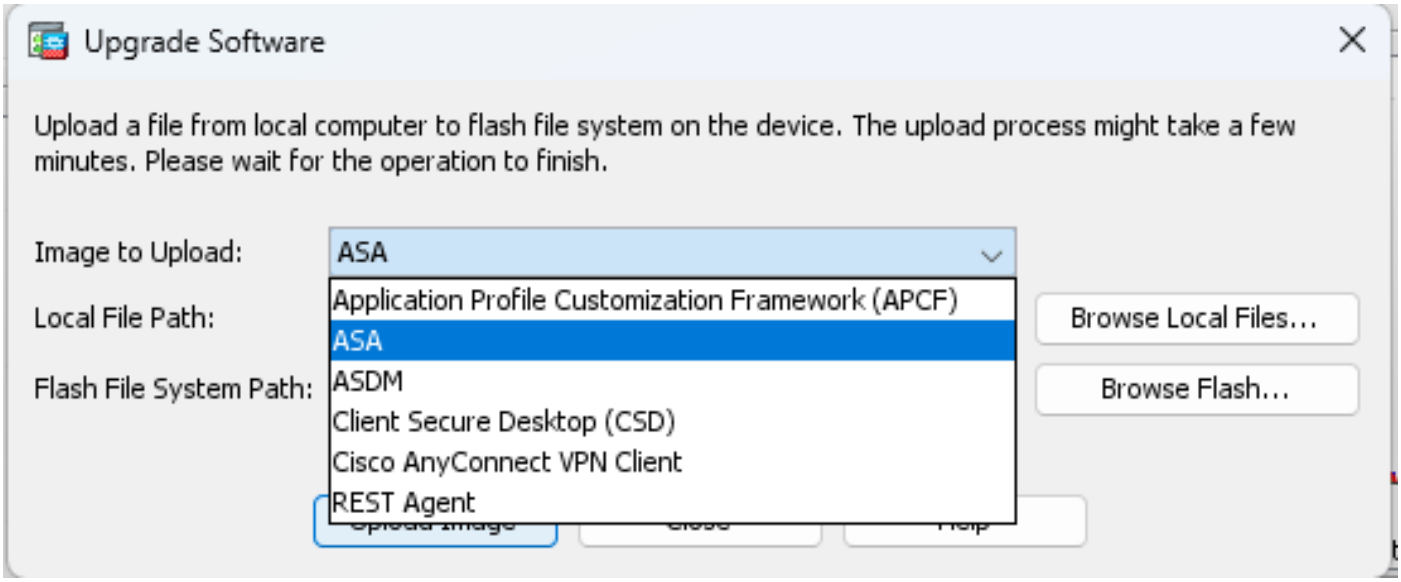
步骤1:使用ASDM连接到辅助设备。



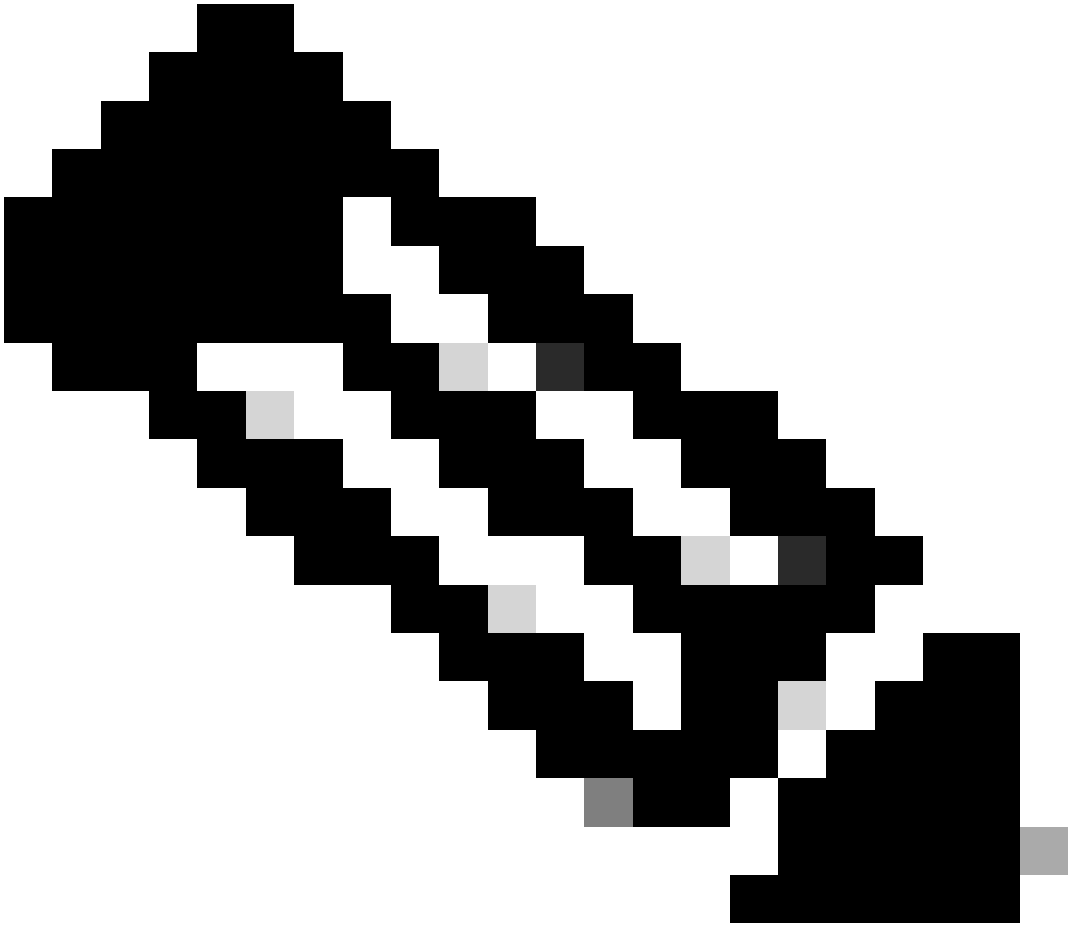
第二步：转至Tools > Upgrade Software from Local Computer。



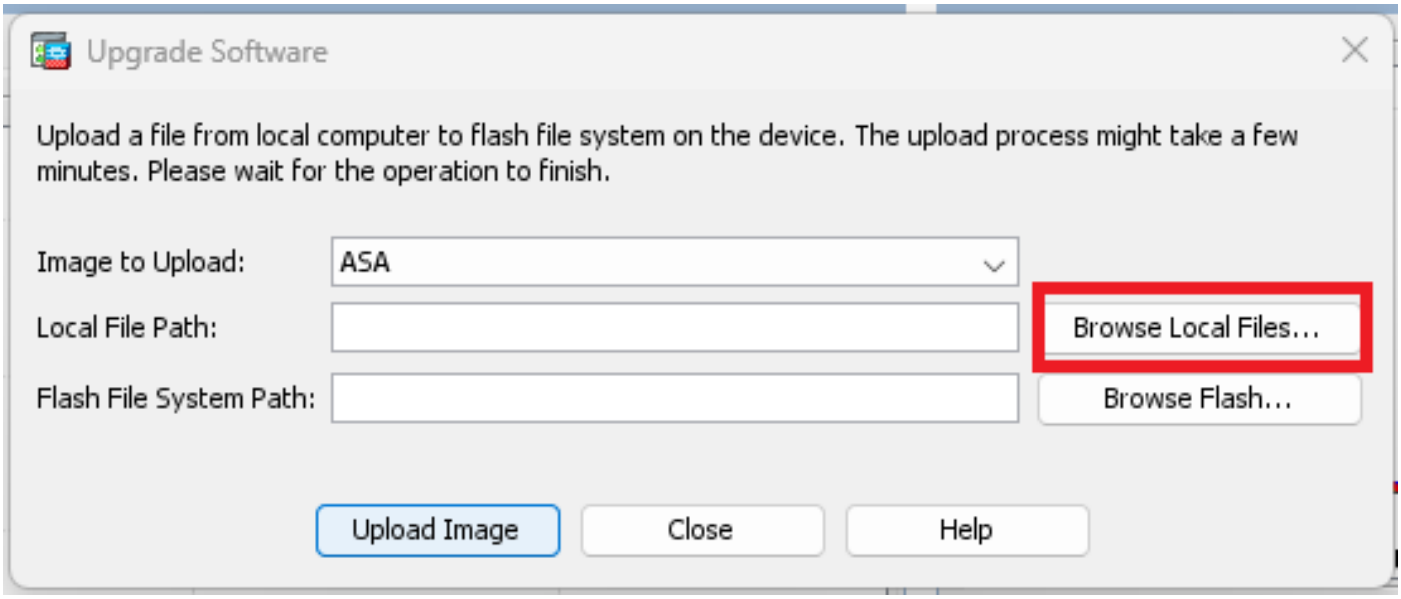
第三步：从下拉列表中选择ASA。



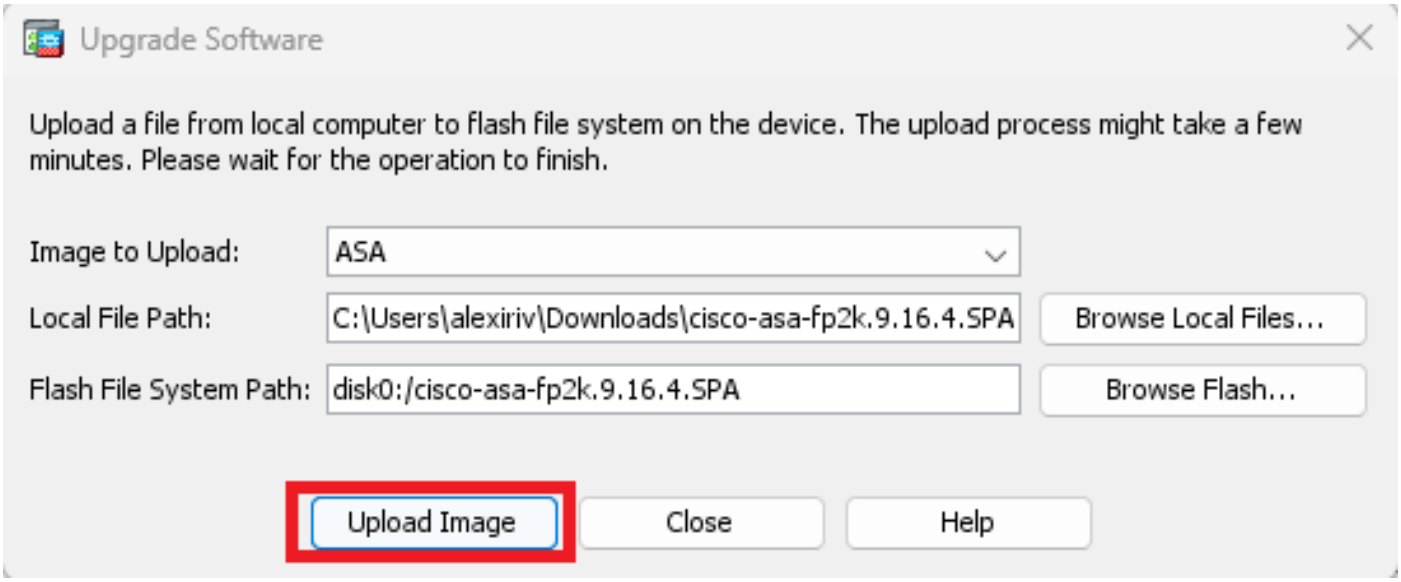
第四步：在升级软件窗口中，单击浏览本地文件以将软件映像上传到辅助单元。



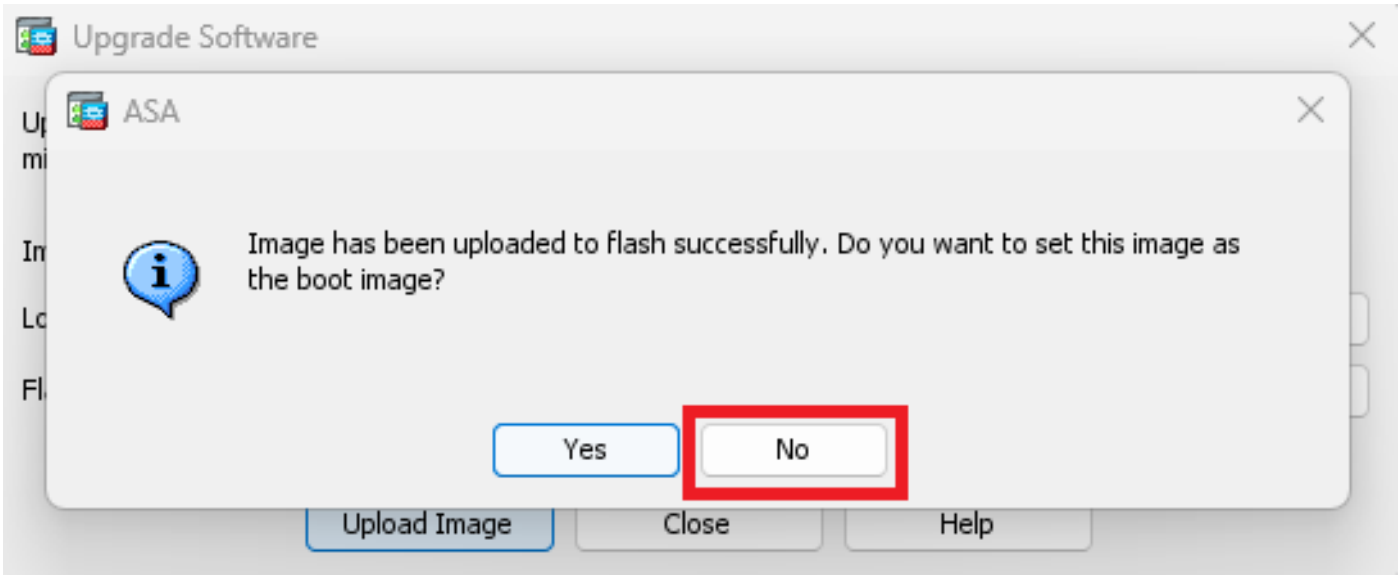
注意：默认情况下，**Flash File System Path**为disk0；要更改路径，请单击**Browse Flash**并选择新路径。



点击**上传图像**。



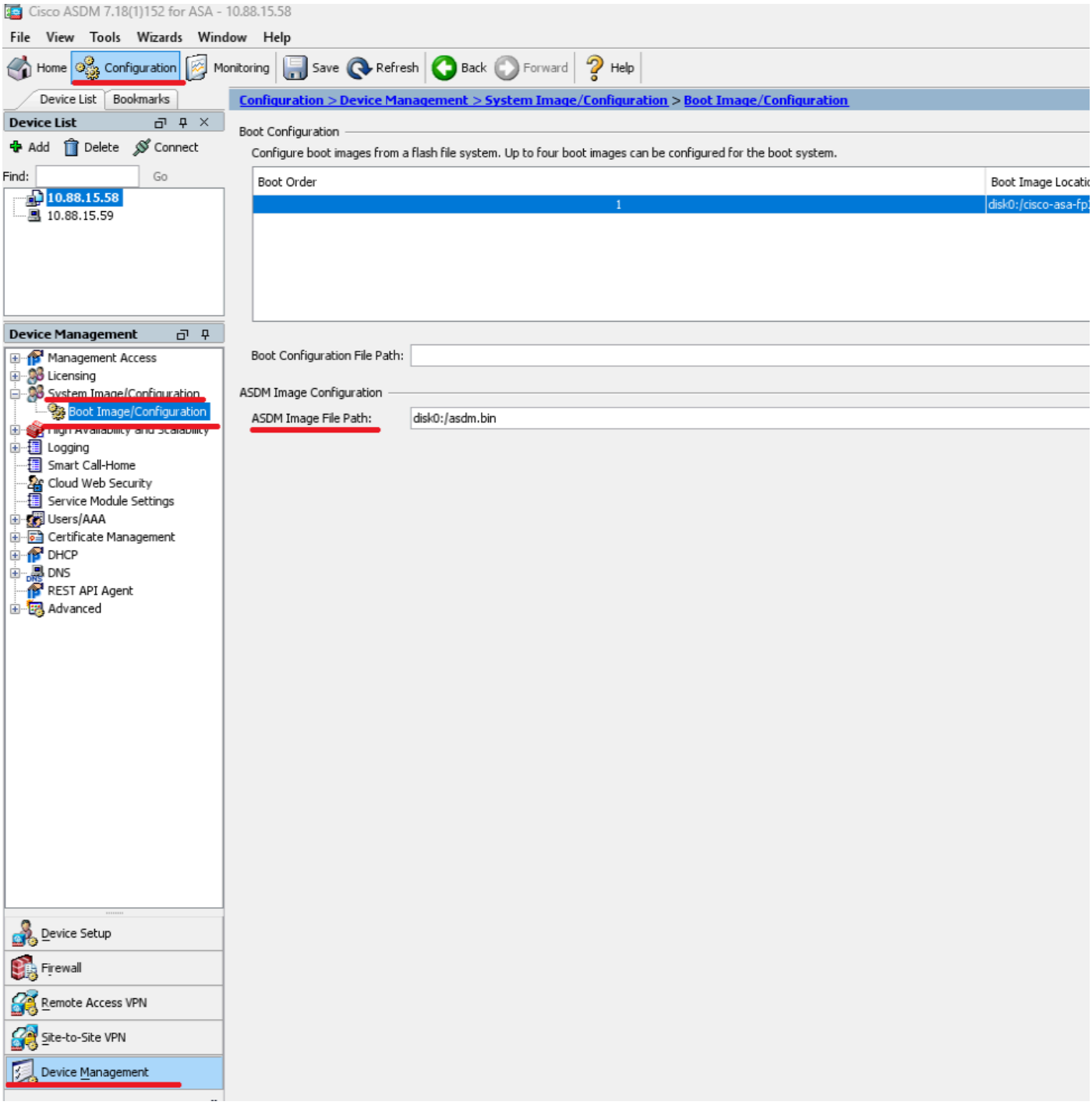
上传映像完成后，点击**否**。



第五步：重置ASDM映像。

使用ASDM连接到主设备并转至**Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration**。

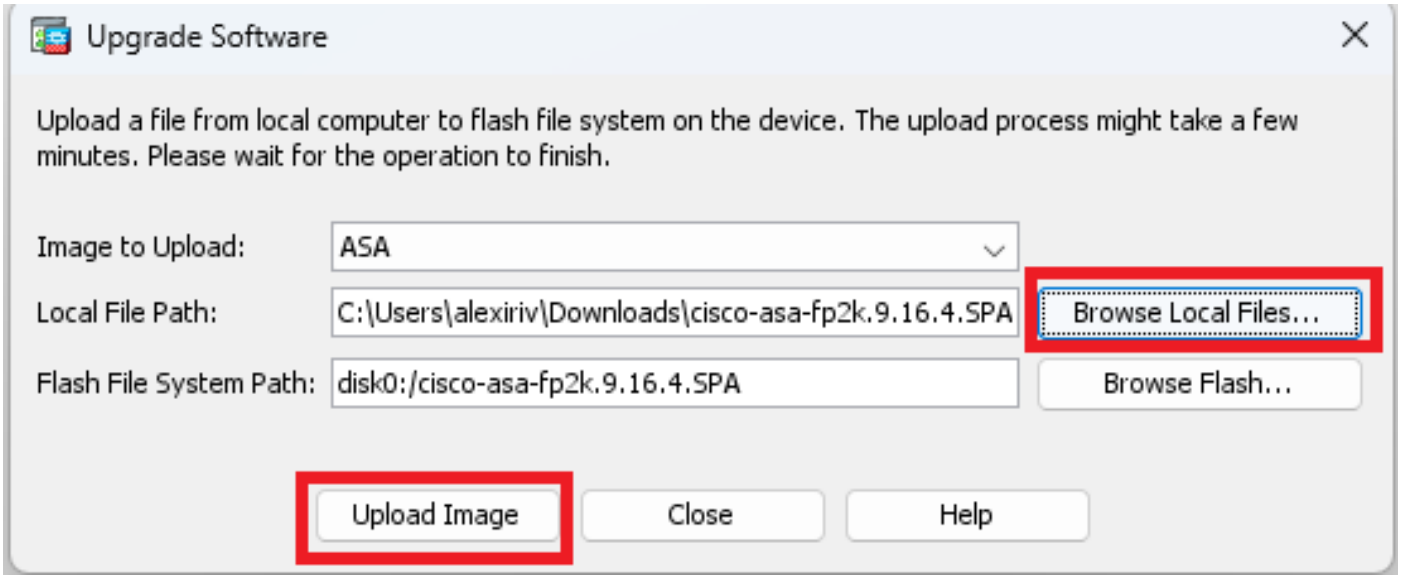
在**ASDM Image File Path**中，输入值**disk0：/asdm.bin**，然后单击**Apply**。



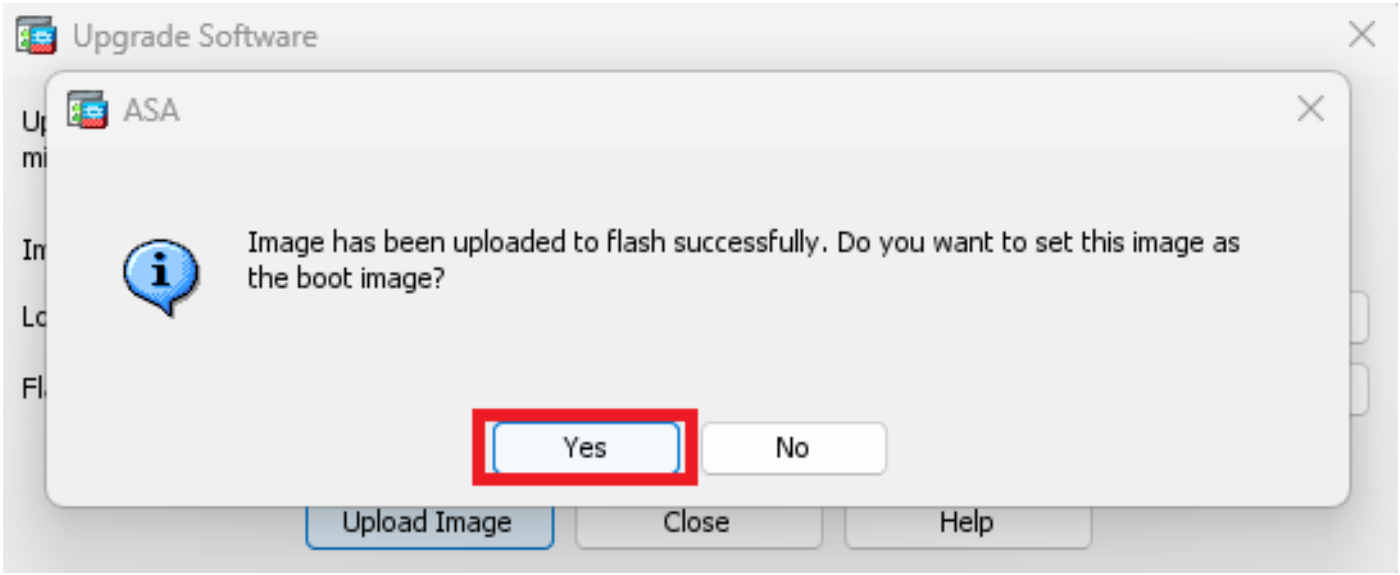
第六步： 将软件映像上传到主设备。

单击**Browse Local Files**，然后选择您设备上的升级包。

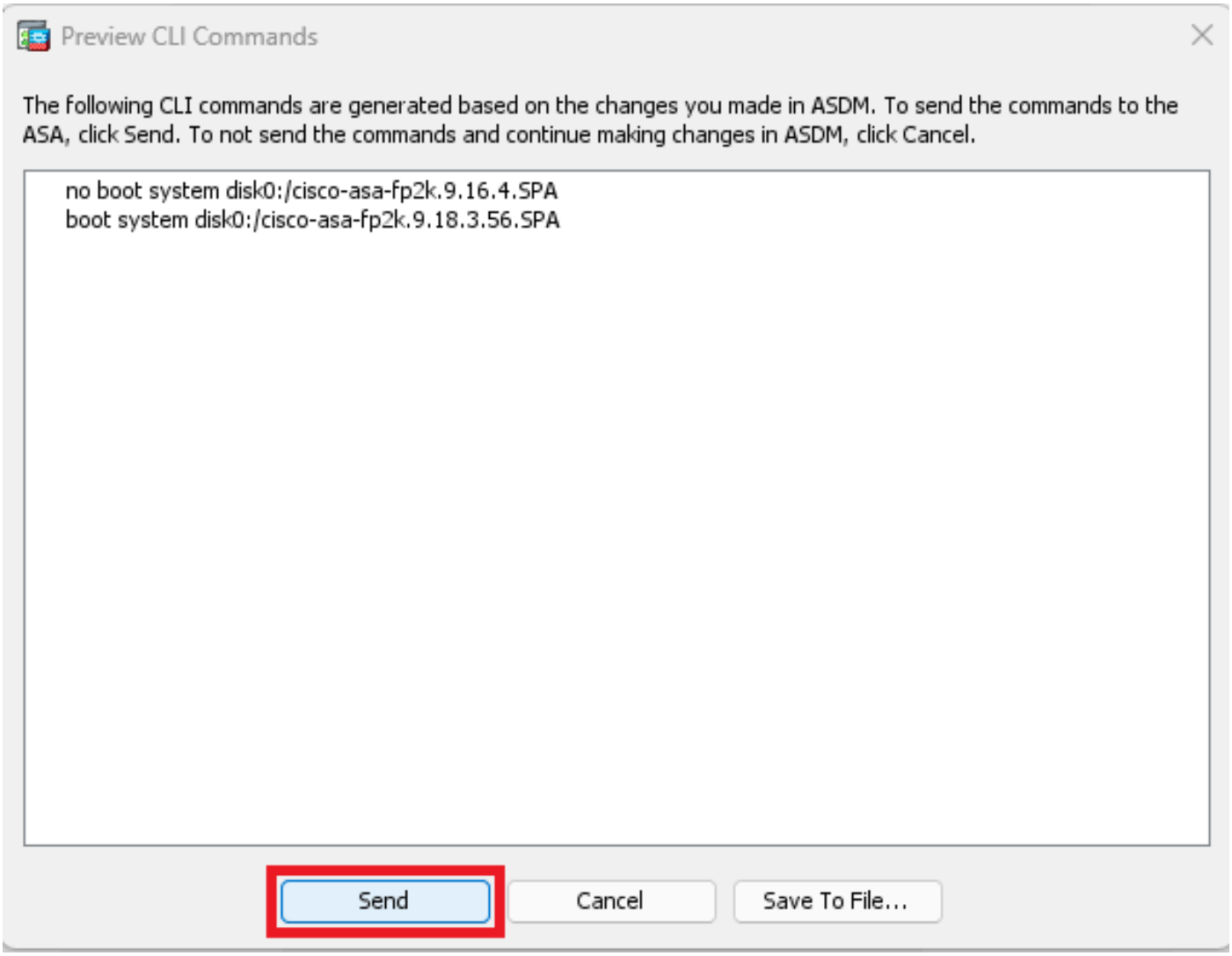
点击**上传图像**。



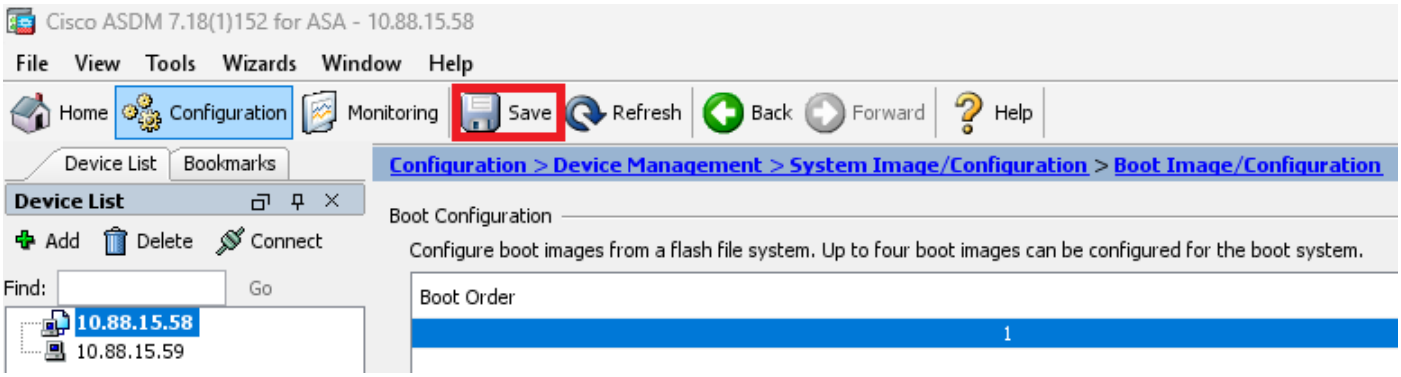
上传完映像后，单击**Yes**。



在预览窗口中，单击**Send**按钮保存配置。

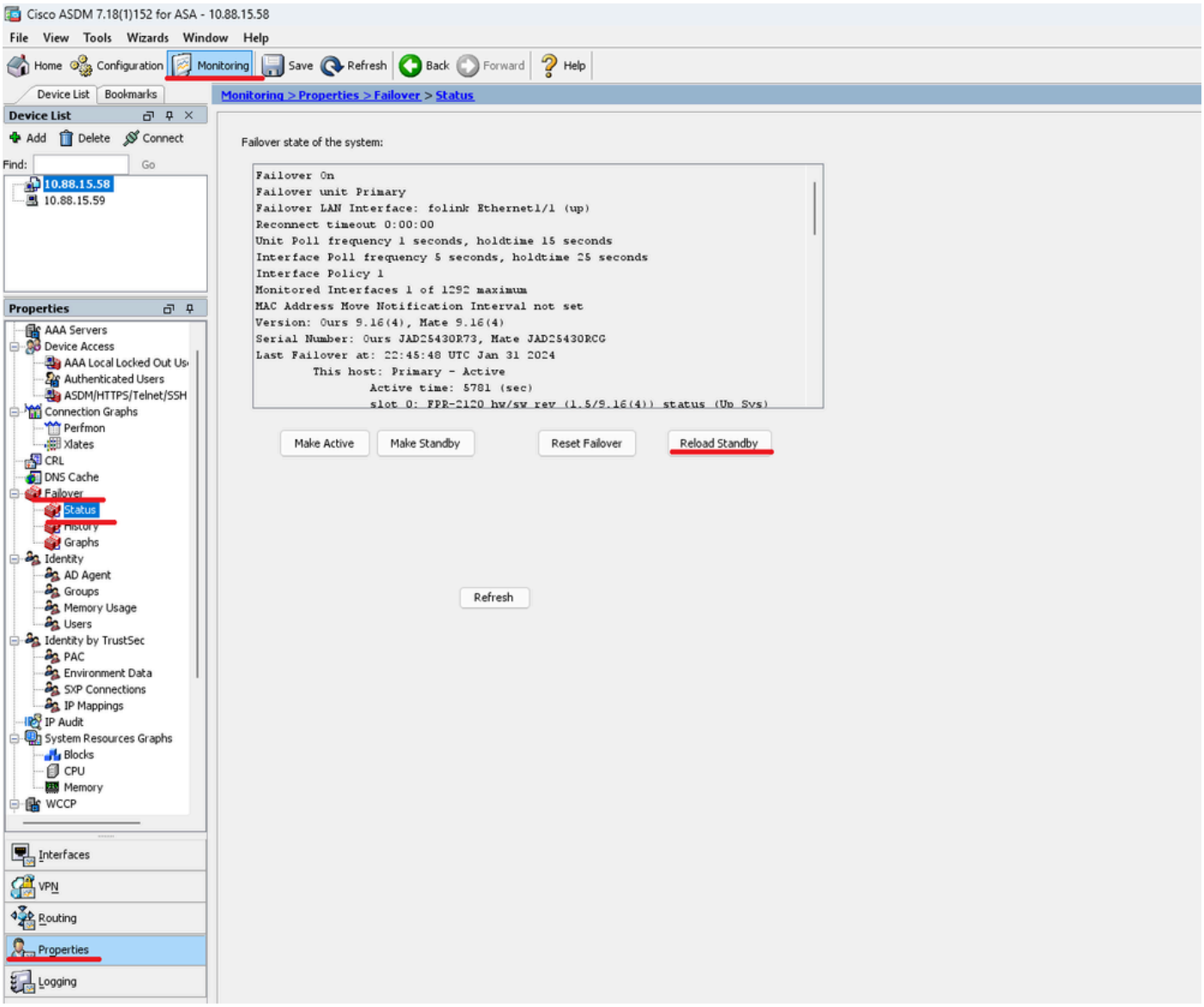


步骤 7. 单击**Save**保存配置。



步骤 8 重新加载辅助设备以安装新版本。

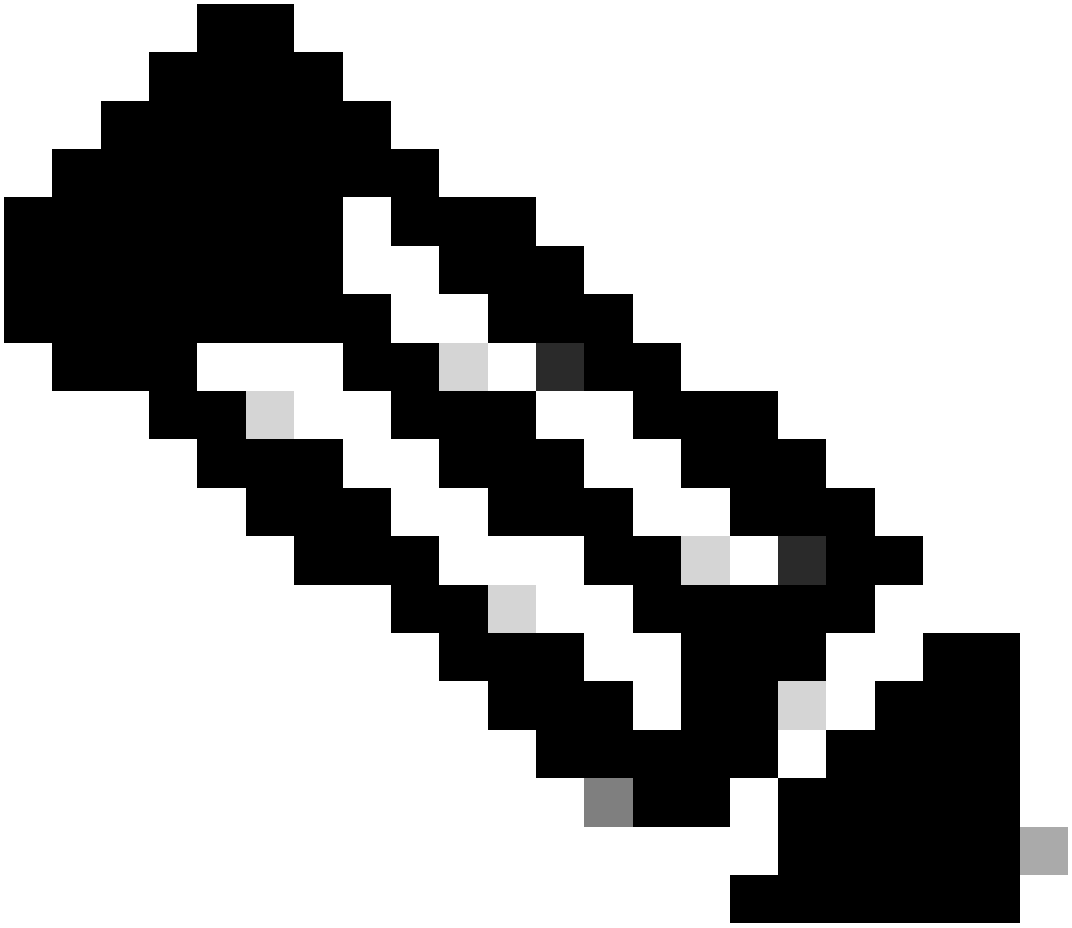
转至Monitoring > **Properties** > **Failover** > **Status**，然后单击**Reload Standby**。



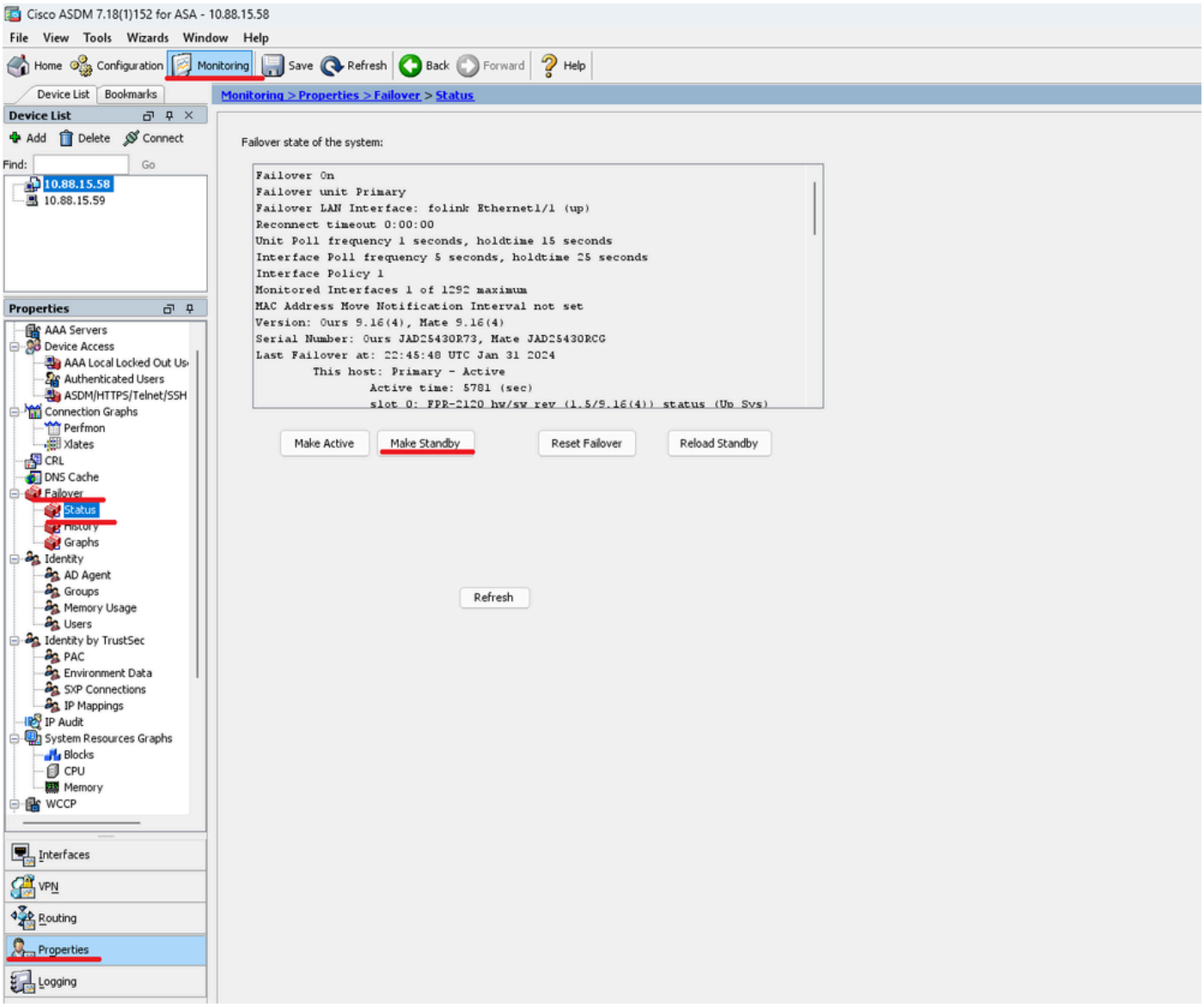
等待备用设备加载。

步骤 9备用设备重新加载后，将主设备从主用状态更改为备用状态。

转至Monitoring > **Properties** > **Failover** > **Status**，然后单击**Make Standby**。

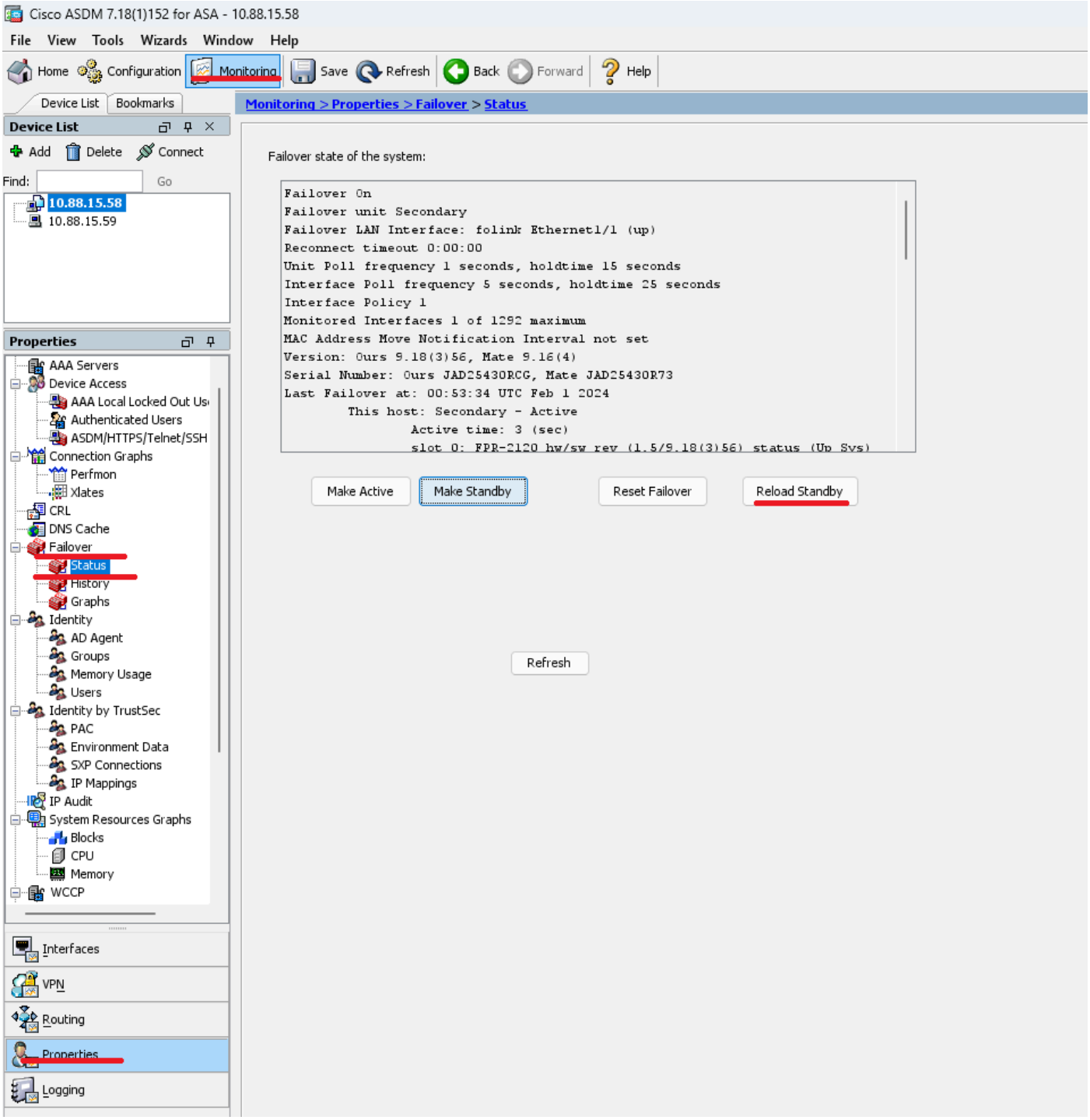


注意：ASMD自动连接到新的主用设备。



步骤 10重新加载新的备用设备以安装新版本。

转至Monitoring > **Properties** > **Failover** > **Status**，然后单击**Reload Standby**。



加载新的备用设备后，升级完成。

验证

要验证两台设备上的升级是否已完成，请通过CLI和ASDM检查升级。

通过CLI

```
<#root>

ciscoasa#
```

show failover

```
Failover On
Failover unit Primary
Failover LAN Interface: folink Ethernet1/1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1292 maximum
MAC Address Move Notification Interval not set
```

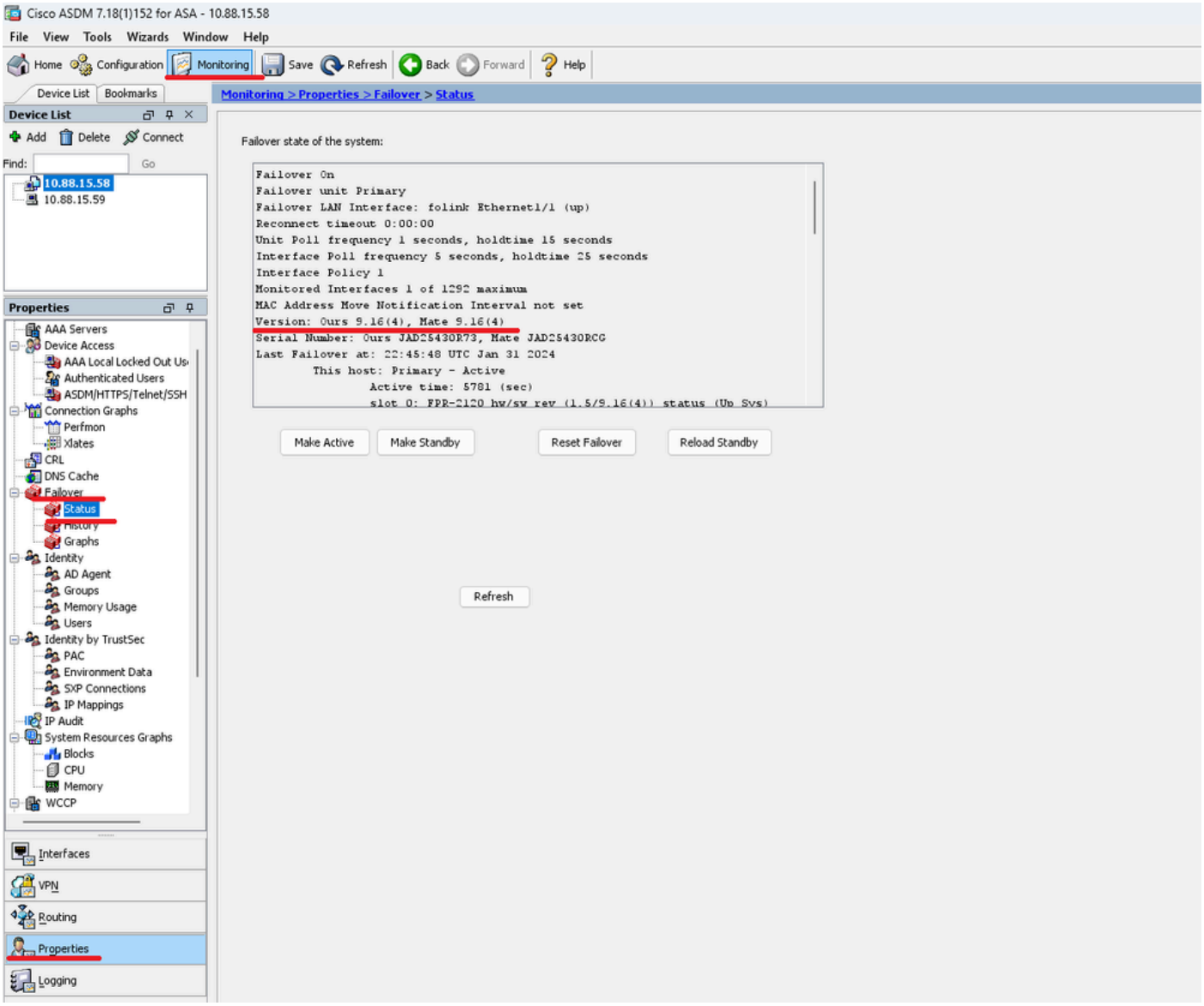
Version: Ours 9.16(4), Mate 9.16(4)

```
Serial Number: Ours JAD25430R73, Mate JAD25430RCG
Last Failover at: 22:45:48 UTC Jan 31 2024
This host: Primary - Active
Active time: 45 (sec)
slot 0: FPR-2120 hw/sw rev (1.5/9.16(4)) status (Up Sys)
Interface management (10.88.15.58): Normal (Monitored)
Other host: Secondary - Standby Ready
Active time: 909 (sec)
slot 0: FPR-2120 hw/sw rev (1.5/9.16(4)) status (Up Sys)
Interface management (10.88.15.59): Normal (Monitored)

Stateful Failover Logical Update Statistics
Link : folink Ethernet1/1 (up)
Stateful Obj xmit xerr rcv rerr
General 27 0 29 0
sys cmd 27 0 27 0
up time 0 0 0 0
RPC services 0 0 0 0
TCP conn 0 0 0 0
UDP conn 0 0 0 0
ARP tbl 0 0 1 0
Xlate_Timeout 0 0 0 0
IPv6 ND tbl 0 0 0 0
VPN IKEv1 SA 0 0 0 0
VPN IKEv1 P2 0 0 0 0
VPN IKEv2 SA 0 0 0 0
VPN IKEv2 P2 0 0 0 0
VPN CTCP upd 0 0 0 0
VPN SDI upd 0 0 0 0
VPN DHCP upd 0 0 0 0
SIP Session 0 0 0 0
SIP Tx 0 0 0 0
SIP Pinhole 0 0 0 0
Route Session 0 0 0 0
Router ID 0 0 0 0
```

```
User-Identity 0 0 1 0
CTS SGTNAME 0 0 0 0
CTS PAC 0 0 0 0
TrustSec-SXP 0 0 0 0
IPv6 Route 0 0 0 0
STS Table 0 0 0 0
Umbrella Device-ID 0 0 0 0

Logical Update Queue Information
Cur Max Total
Recv Q: 0 10 160
Xmit Q: 0 1 53
```

通过ASDM

转至**Monitoring** > **Properties** > **Failover** > **Status**，您可以看到两个设备的ASA版本。



相关信息

- 思科安全防火墙ASA兼容性
- 思科安全防火墙ASA升级指南

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）。