将安全防火墙ASA调配到CSM

目录

简介

本文档介绍向思科安全管理器(CSM)调配安全防火墙自适应安全设备(ASA)的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全防火墙ASA
- CSM

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全防火墙ASA版本9.18.3
- CSM版本4.28

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

CSM有助于实现一致的策略实施，并快速排除安全事件的故障，从而提供涵盖整个安全部署的摘要报告。借助其集中式界面，组织可以高效扩展和管理各种思科安全设备，同时提高可视性。

配置

在下一个示例中，虚拟ASA调配到CSM以进行集中管理。

配置

为HTTPS管理配置ASA

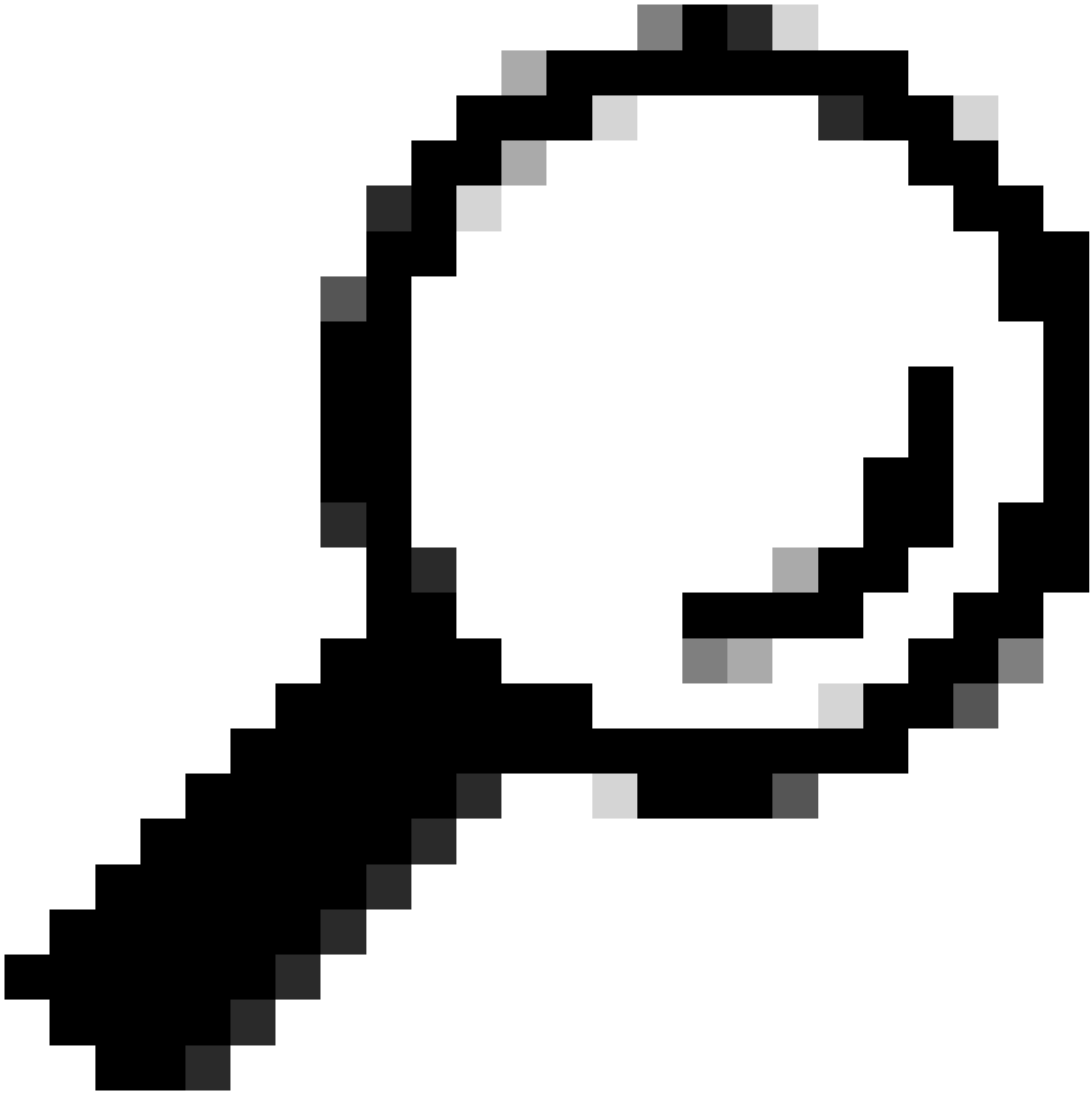
步骤1:创建具有所有权限的用户。

命令行(CLI)语法：

```
configure terminal
username < user string > password < password > privilege < level number >
```

这转换为下一个命令示例，其中包含了用户csm-user和口令cisco123，如下所示：

```
ciscoasa# configure terminal
ciscoasa(config)# username csm-user password cisco123 privilege 15
```



提示：外部身份验证用户也用于此集成。

第二步：启用HTTP服务器。

命令行(CLI)语法：

```
configure terminal
http server enable
```

第三步：允许CSM服务器IP地址进行HTTPS访问。

命令行(CLI)语法：

```
configure terminal
http < hostname > < netmask > < interface name >
```

这转换为下一个命令示例，该示例允许任何网络通过外部接口(GigabitEthernet0/0)上的HTTPS访问ASA：

```
ciscoasa# configure terminal
ciscoasa(config)# http 0.0.0.0 0.0.0.0 outside
```

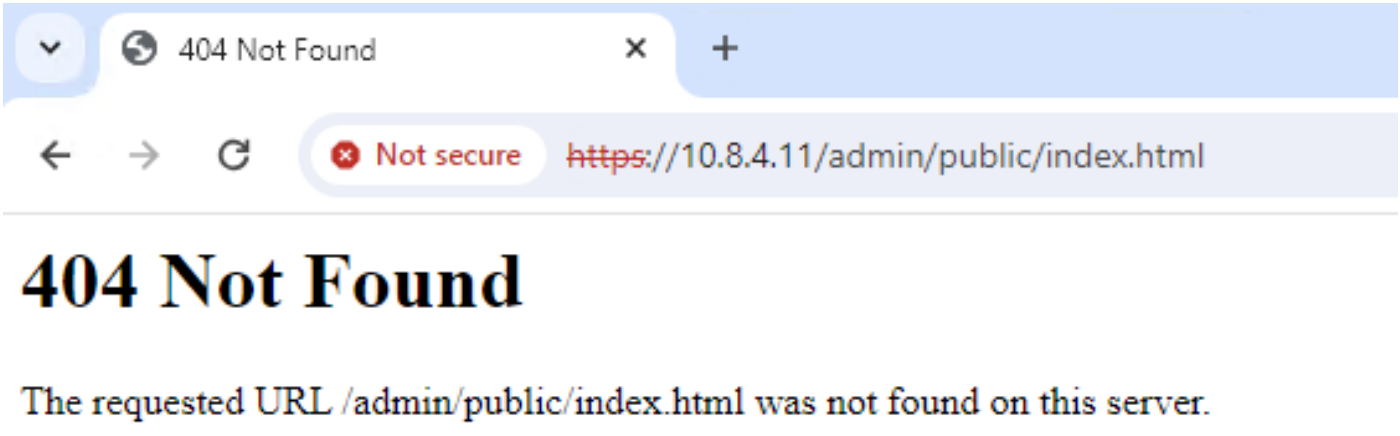
第四步：验证从CSM服务器可以访问HTTPS。

打开任何Web浏览器并键入下一个语法：

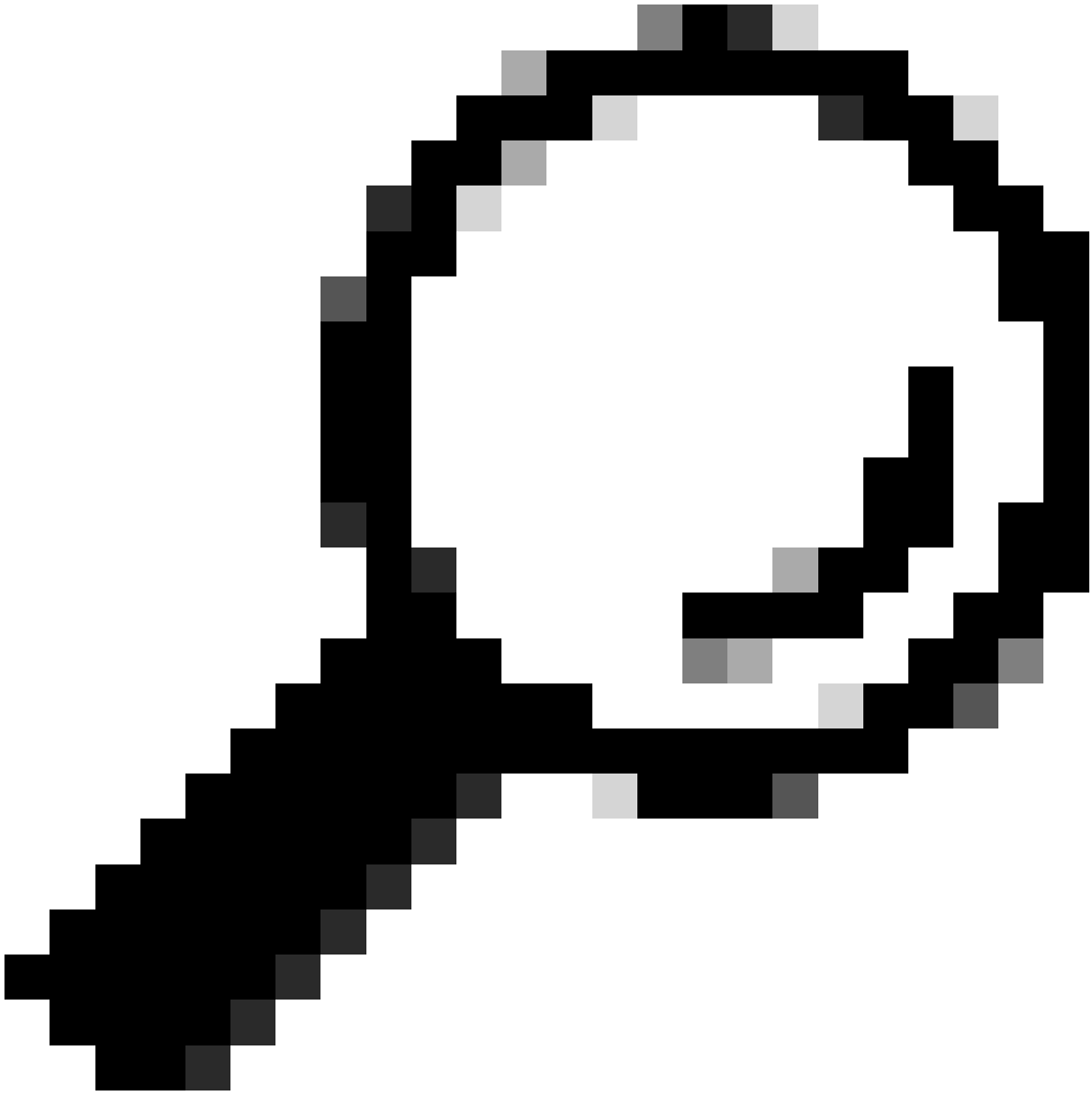
```
https://< ASA IP address >/
```

这转换为在上一步中允许HTTPS访问的外部接口IP地址的下一个示例：

```
https://10.8.4.11/
```



ASA HTTPS响应



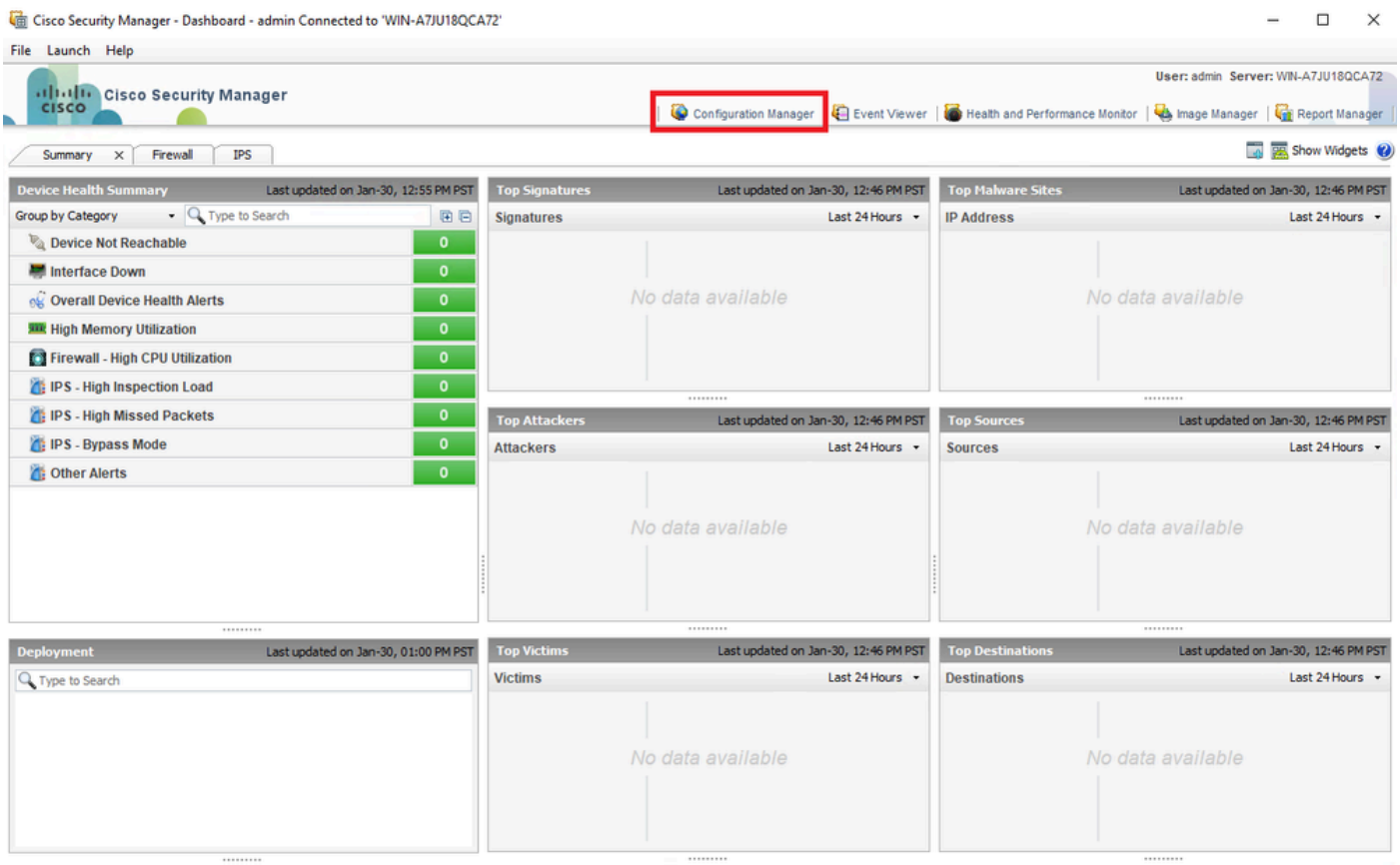
提示：Error 404 Not Found expected on this step，因为此ASA未安装思科自适应安全设备管理器(ASDM)，但是页面重定向到URL /admin/public/index.html时存在HTTPS响应。

将安全防火墙ASA调配到CSM

步骤1:打开并登录到CSM客户端。

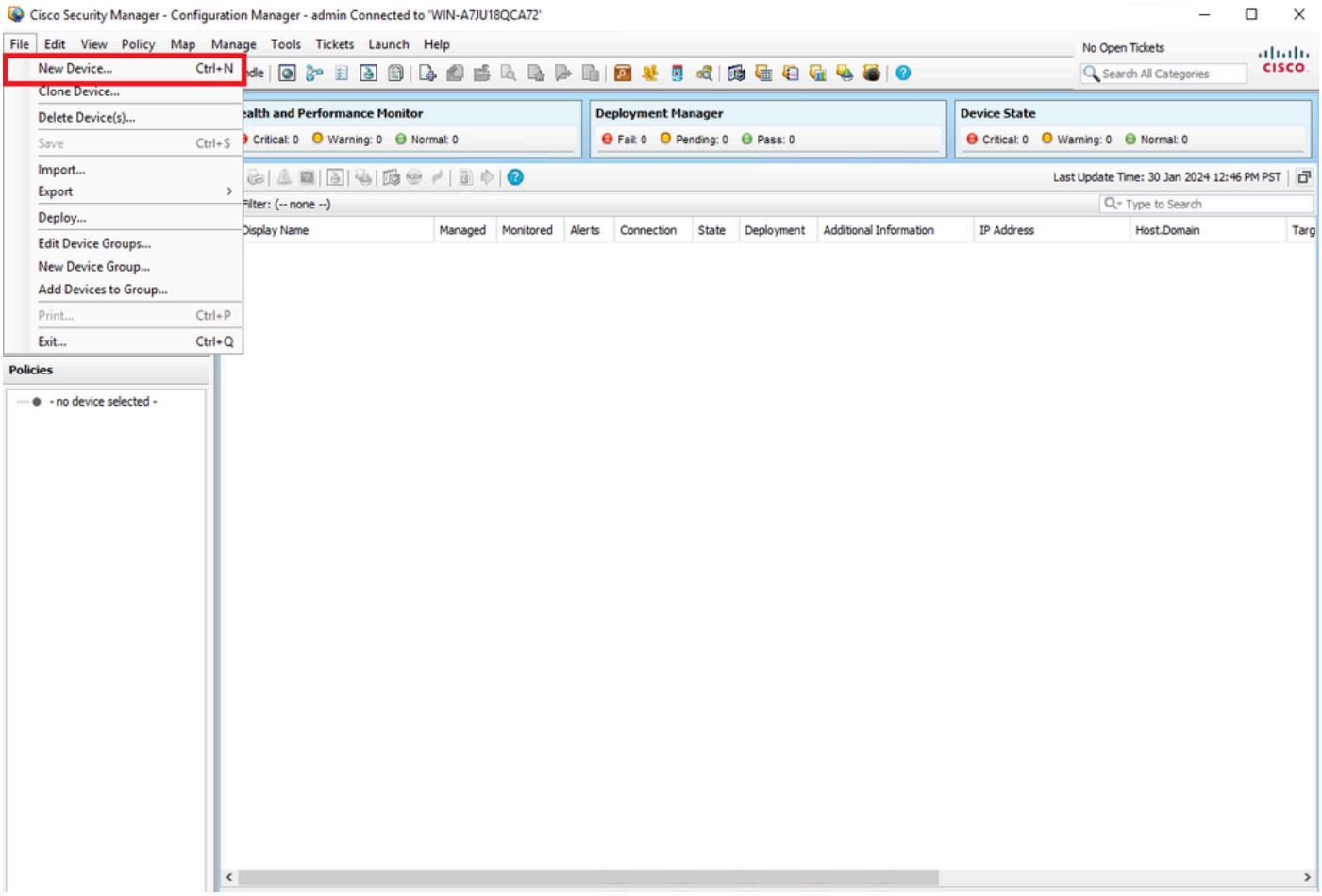
CSM客户端登录

第二步：打开Configuration Manager。



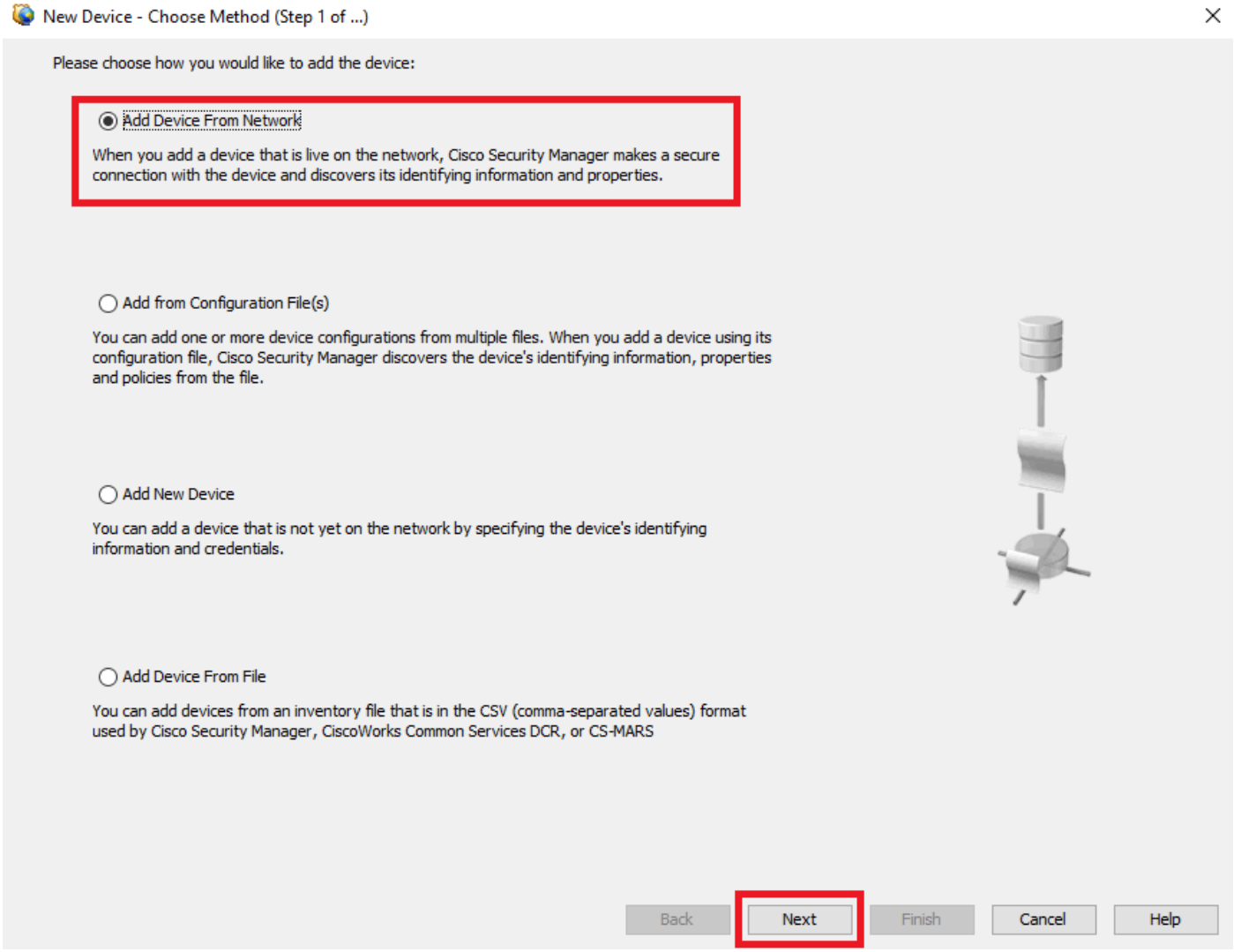
CSM客户端控制面板

第三步：导航到设备>新设备。



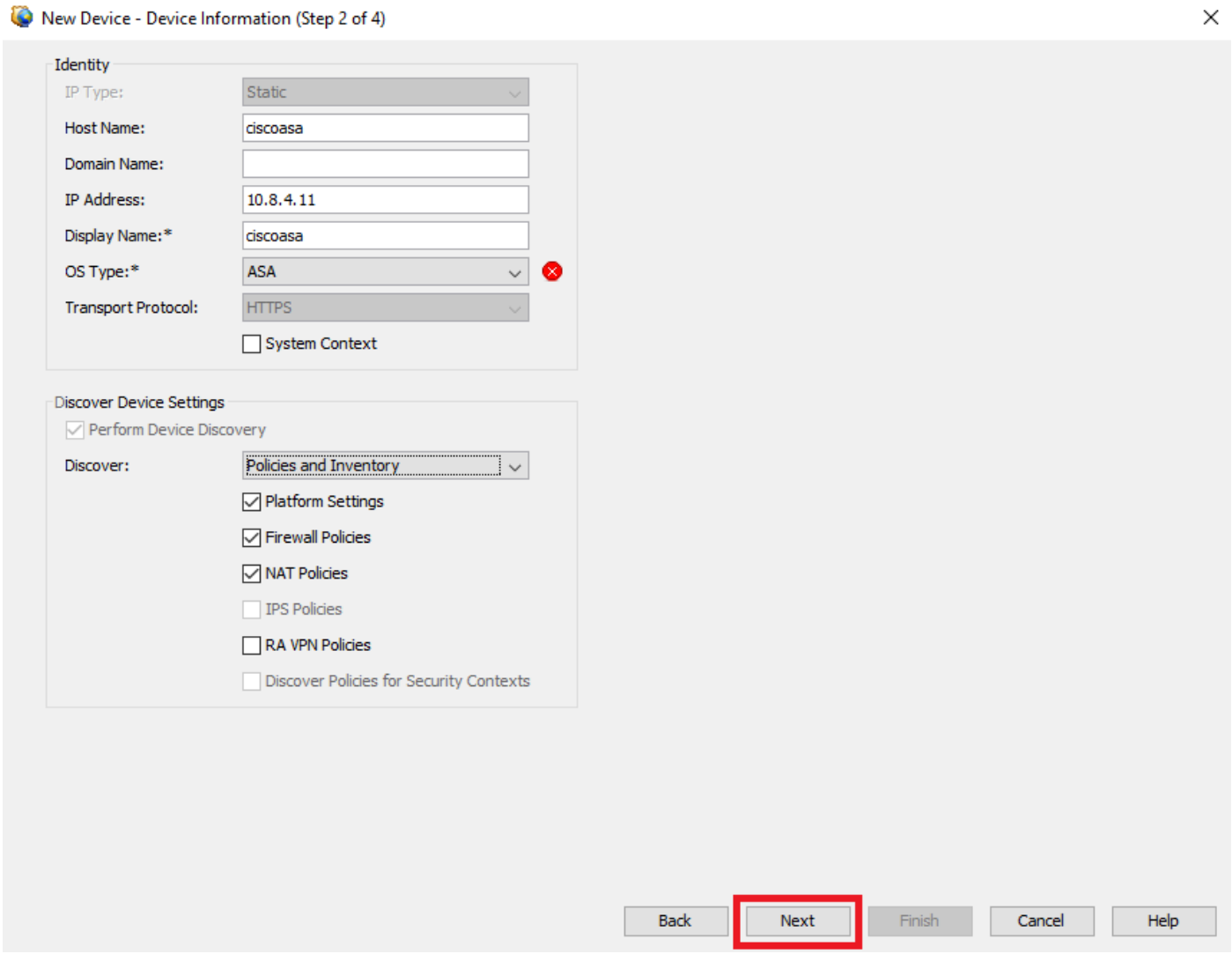
*CSM*配置管理器

第四步：选择根据所需结果满足要求的添加选项。由于网络中已设置配置的ASA，因此本示例的最佳选项是**Add Device From Network**，然后单击**Next**。



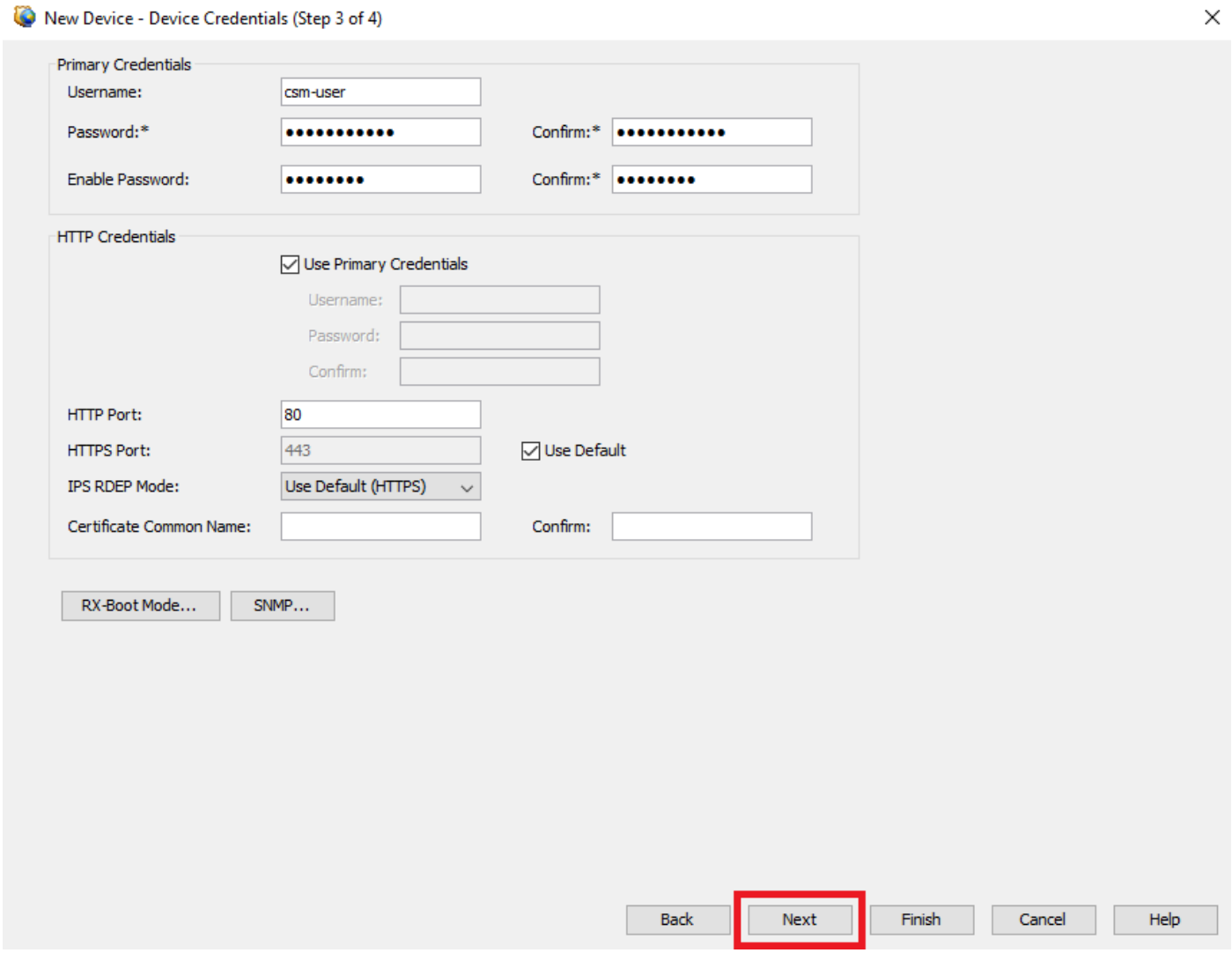
设备添加方法

第五步：根据安全防火墙ASA上的配置和发现设置完成所需数据。然后单击**Next**。



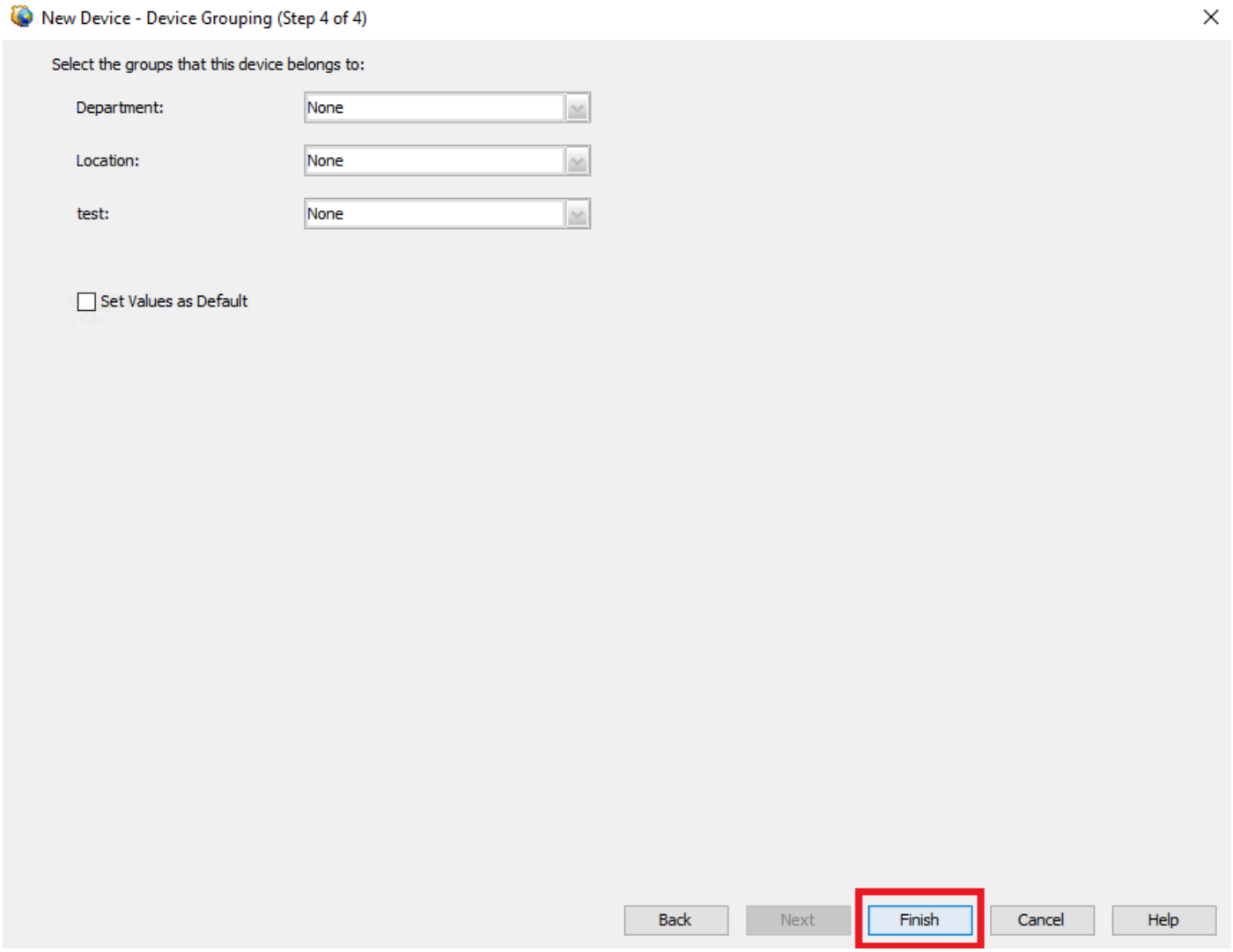
*ASA*设置

第六步：从ASA上配置的CSM用户和**enable**密码完成所需的凭证。



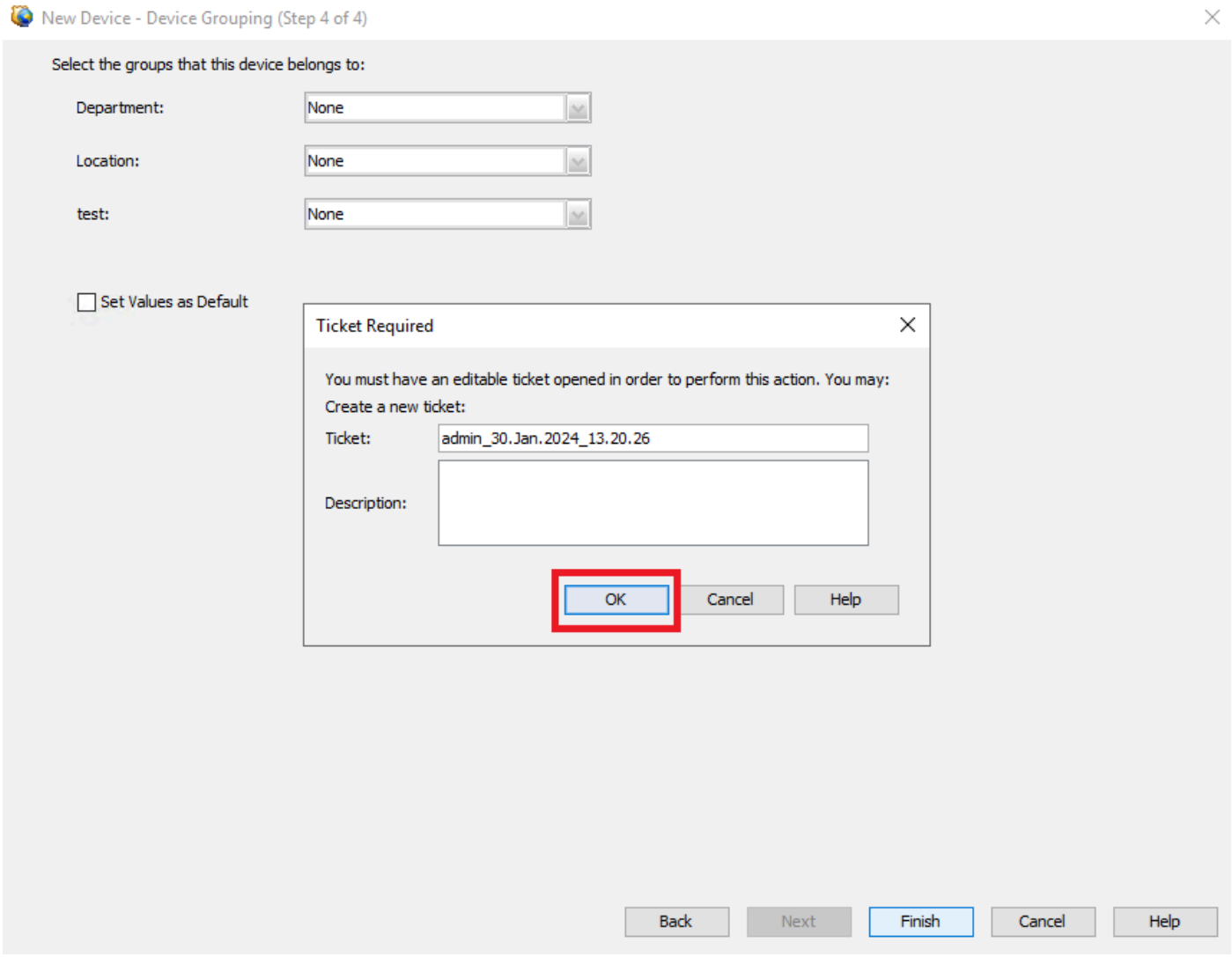
ASA凭证

步骤 7.选择所需的组或在不需要时跳过此步骤，然后单击**Finish**。



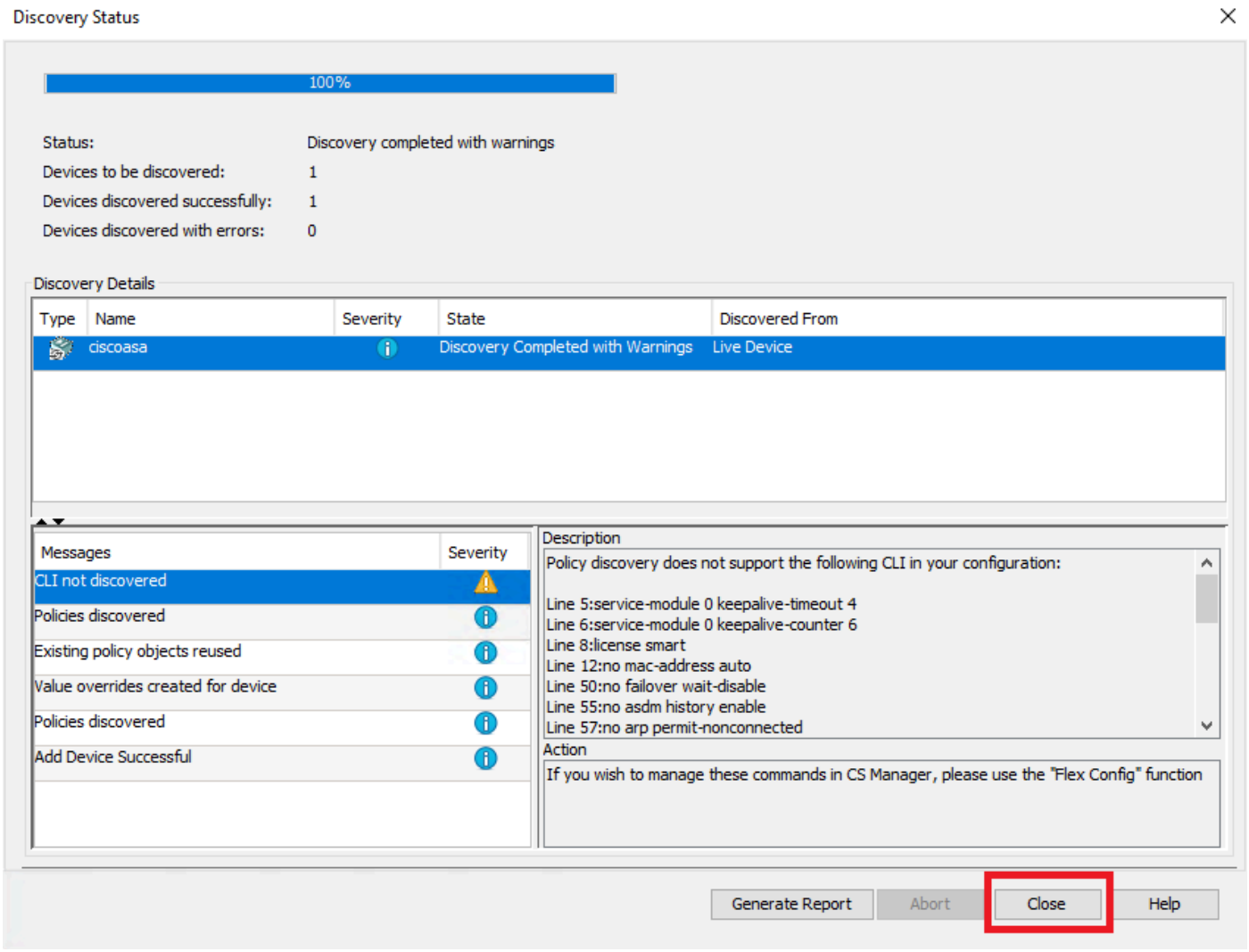
*CSM*组选择

步骤 8出于控制目的而生成票证请求，然后单击**OK**。

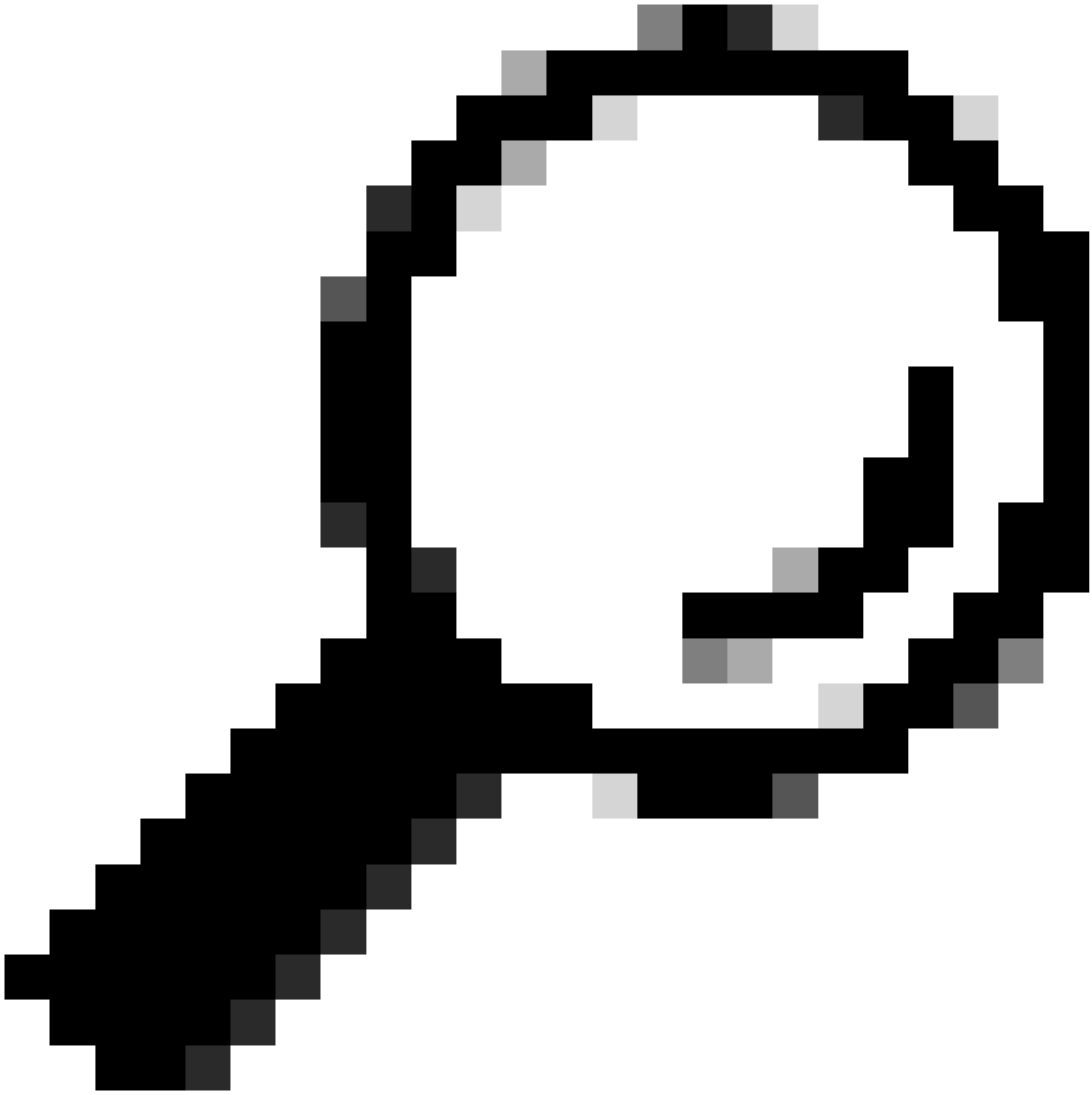


*CSM*票证创建

步骤 9验证发现操作是否完成并且没有错误，然后单击**Close**。

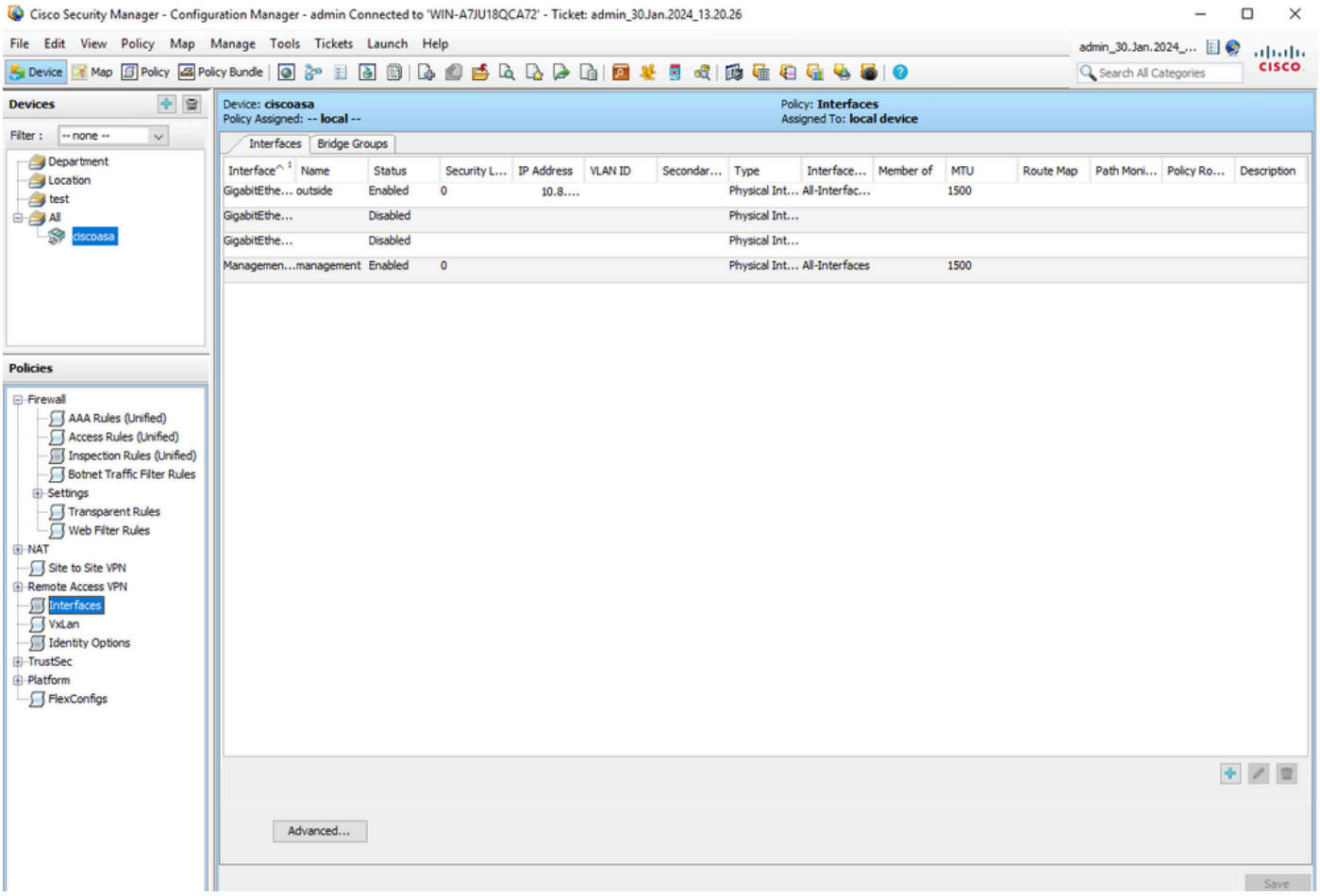

Discovery Status
100%
Status: Discovery completed with warnings
Devices to be discovered: 1
Devices discovered successfully: 1
Devices discovered with errors: 0
Discovery Details
Type Name Severity State Discovered From
ciscoasa Discovery Completed with Warnings Live Device
Messages Severity
CLI not discovered
Policies discovered
Existing policy objects reused
Value overrides created for device
Policies discovered
Add Device Successful
Description
Policy discovery does not support the following CLI in your configuration:
Line 5:service-module 0 keepalive-timeout 4
Line 6:service-module 0 keepalive-counter 6
Line 8:license smart
Line 12:no mac-address auto
Line 50:no failover wait-disable
Line 55:no asdm history enable
Line 57:no arp permit-nonconnected
Action
If you wish to manage these commands in CS Manager, please use the "Flex Config" function
Generate Report
Abort
Close
Help

ASA发现



提示：由于CSM并不支持所有ASA功能，因此警告被接受为成功输出。

步骤 10验证ASA现在显示为已在CSM客户端上注册并显示正确的信息。



已注册*ASA*信息

验证

ASA上提供HTTPS调试用于故障排除。使用下一个命令：

```
debug http
```

以下是CSM注册调试成功的示例：

```
ciscoasa# debug http debug http enabled at level 1. ciscoasa# HTTP: processing handoff to legacy admin
```

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）。