17. Cisco Firepower 与ISE PIC整合实战

教主VIP，聊点高级的!

教主技术进化论 2022

主讲人：*现任明教教主*

北京乾颐堂网络实验室出品

1. ISE PIC技术介绍
2. 环境介绍
3. AD, FMC, ISE整合
4. FMC策略

1. ISE PIC技术介绍

ISE-PIC Overview

Passive Identity Connector (ISE-PIC) offers a centralized, one-stop installation and implementation enabling you to easily and simply configure your network in order to receive and share user identity information[接收并分享用户身份信息给不同的安全产品] with a variety of different security product subscribers such as Cisco Firepower Management Center (FMC) and Stealthwatch. As the full broker for passive identification, ISE-PIC collects user identities from different provider sources, such as Active Directory Domain Controllers (AD DC), maps the user login information to the relevant IP addresses in use and then shares that mapping information with any of the subscriber security products that you have configured.[ISE-PIC从不同的提供源, 例如:AD域控制器, 收集用户登录信息, 并且映射到IP地址, 然后分享给配置的订阅者]

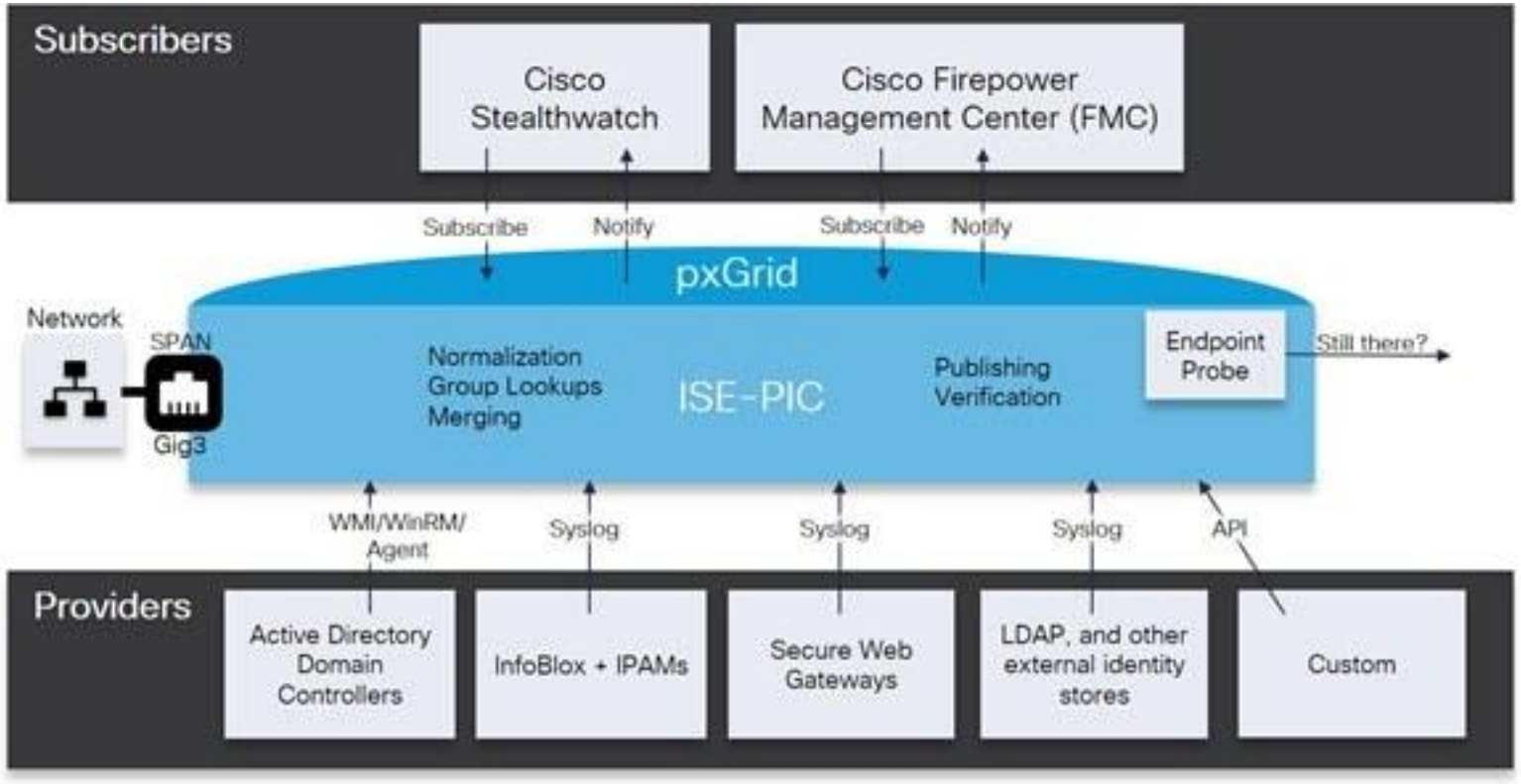
What is Passive Identity?

Products such as the Cisco Identity Services Engine (ISE), which provide an authentication, authorization and accounting (AAA) server, and utilize technologies such as 802.1X or Web Authentication, communicate directly with the user or endpoint[主动认证直接和用户或者终端通信], requesting access to the network, and then using their login credentials in order to verify and actively authenticate their identity.

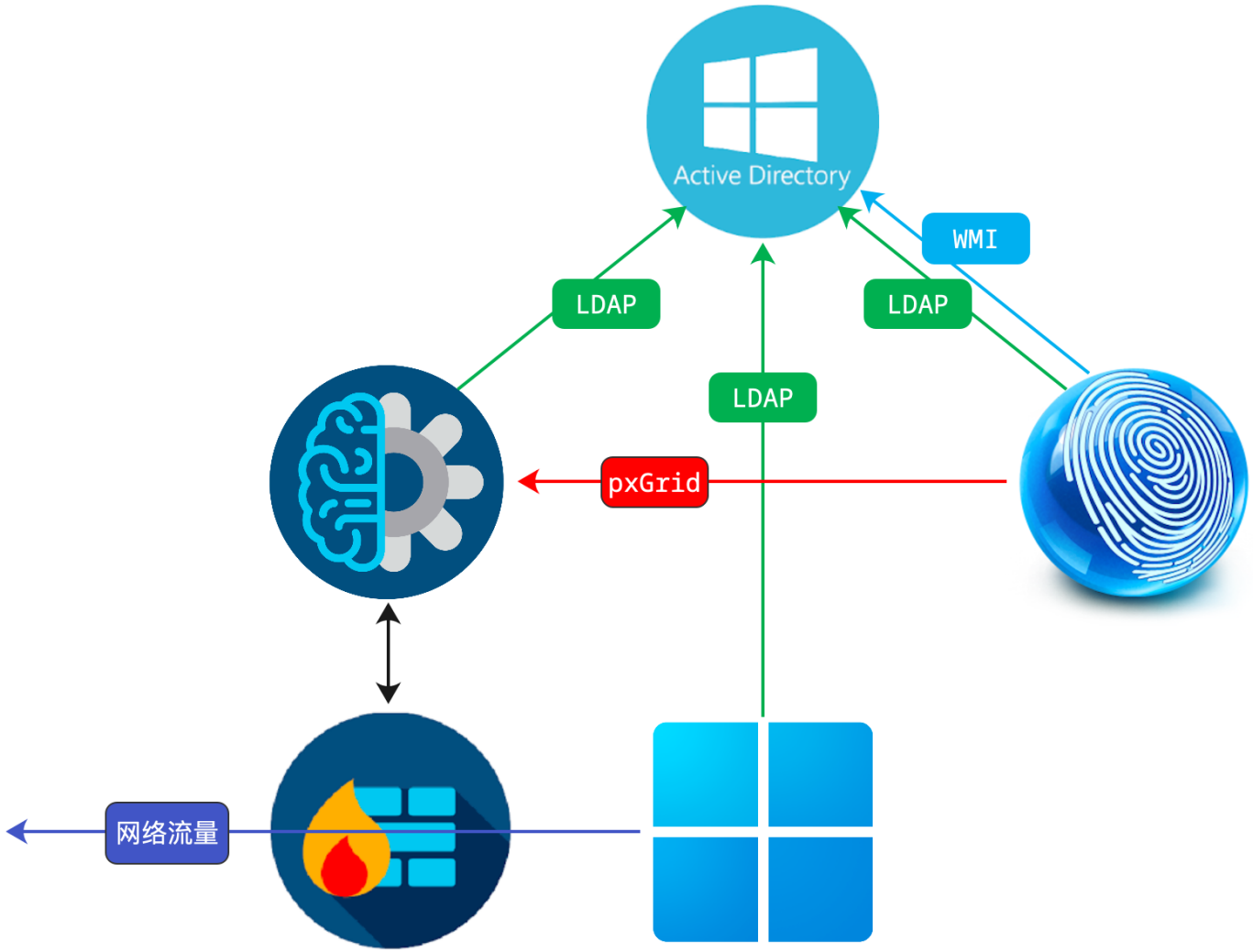
Passive identity services do not authenticate users directly[被动身份服务不直接认证用户], but rather gather user identities and IP addresses from external authentication servers such as Active Directory, known as providers, and then share that information with subscribers[从外部认证服务器, 例如AD, 收集用户和IP信息, 并分享这些信息给订阅者]. ISE-PIC first receives the user identity information from the provider, usually based on the user login and password, and then performs the necessary checks and services in order to match the user identity with the relevant IP address, thereby delivering the authenticated IP address to the subscriber.

Passive Identity Connector (ISE-PIC) Flow

1. Provider performs the authentication of the user or endpoint.
2. Provider sends authenticated user information to ISE-PIC.
3. ISE-PIC normalizes, performs lookups, merges, parses and maps user information to IP addresses and publishes mapped details to pxGrid.
4. pxGrid subscribers receive the mapped user details.



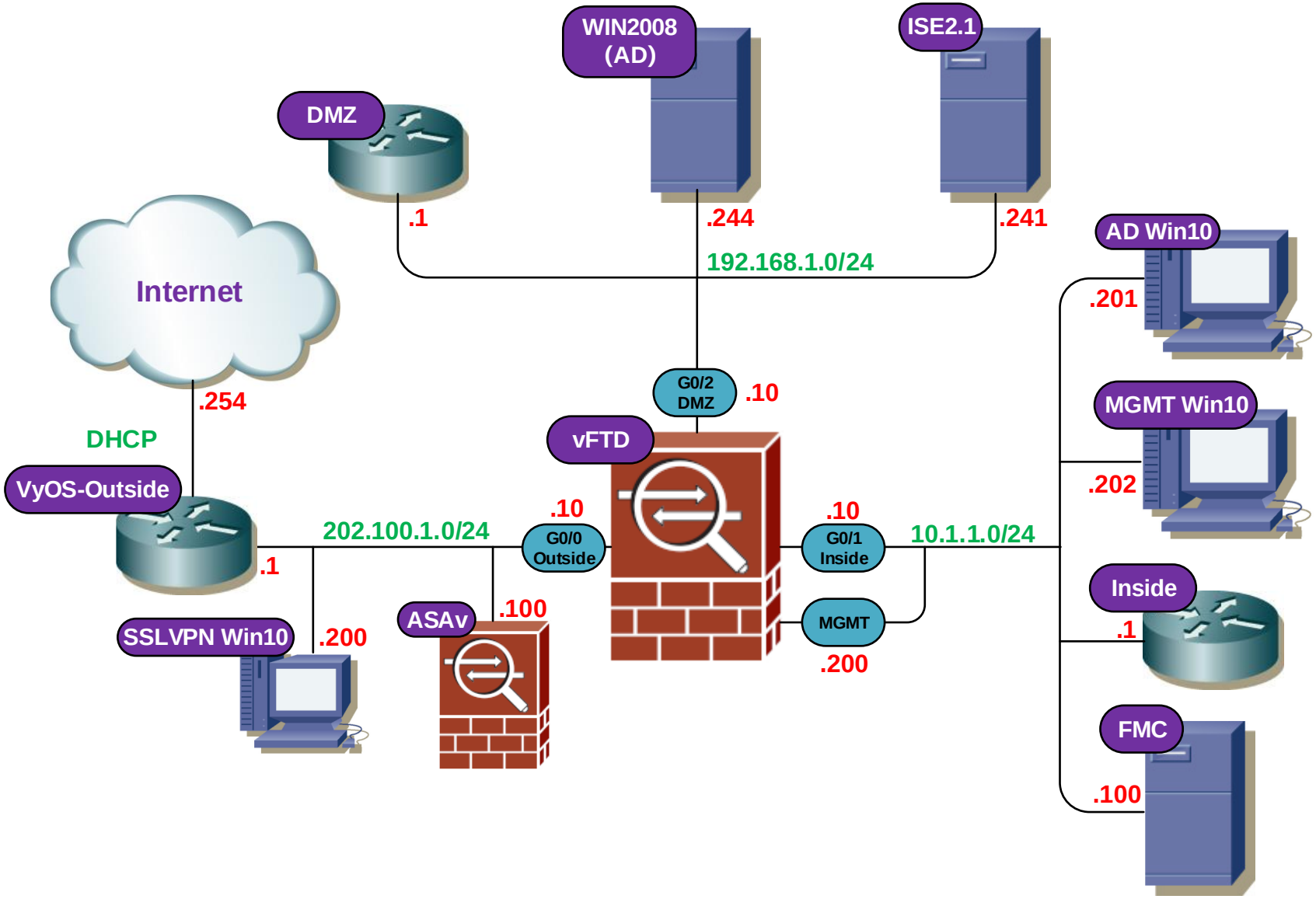
流程示意图



乾颐堂

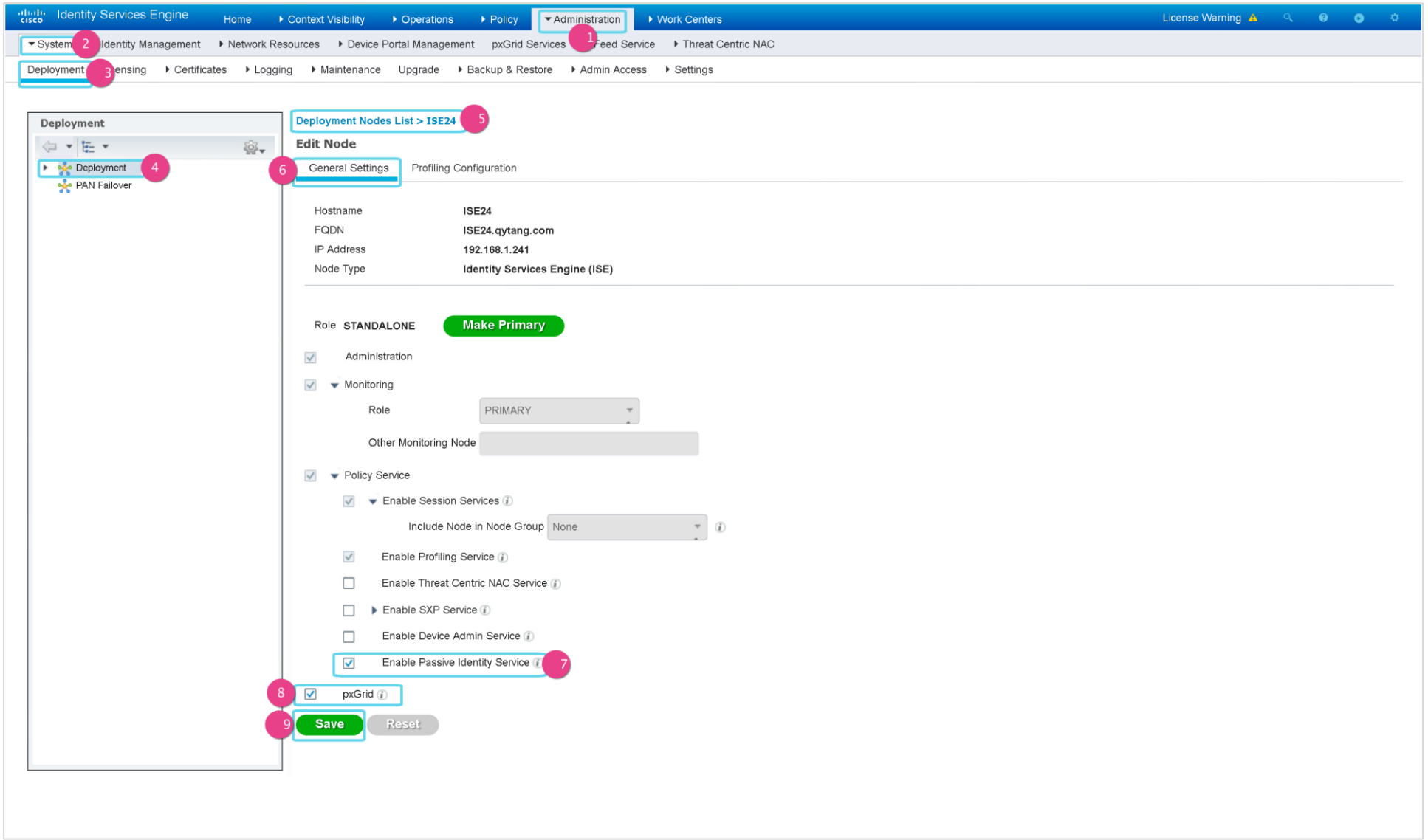
2. 环境介绍

实验拓扑

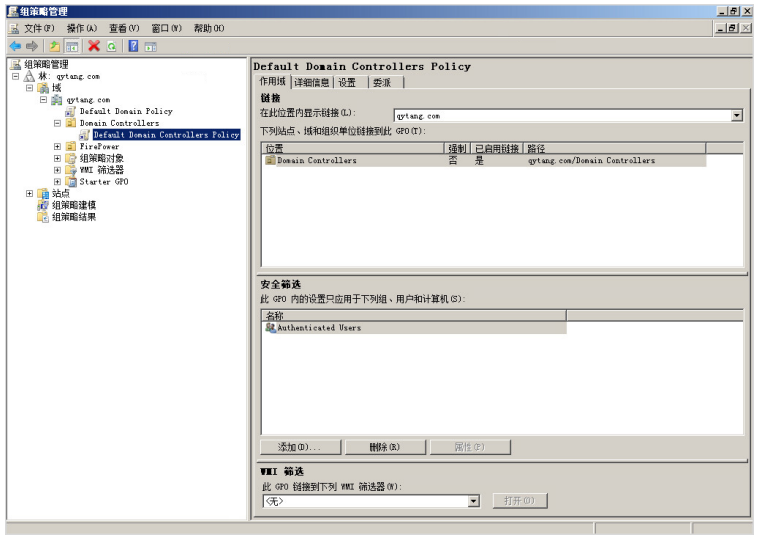


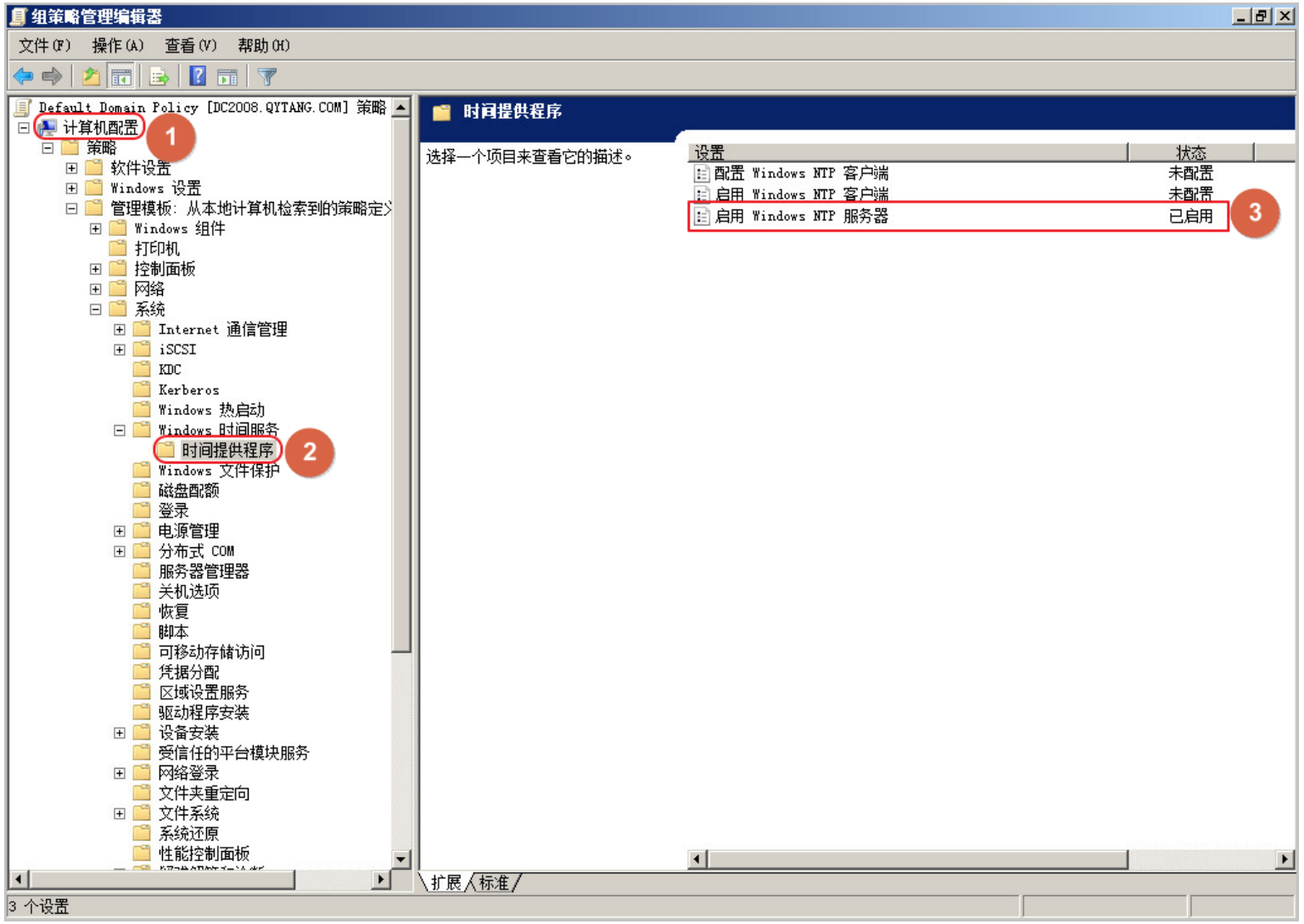
3. AD, FMC, ISE整合

激活pxGrid和Passive ID服务

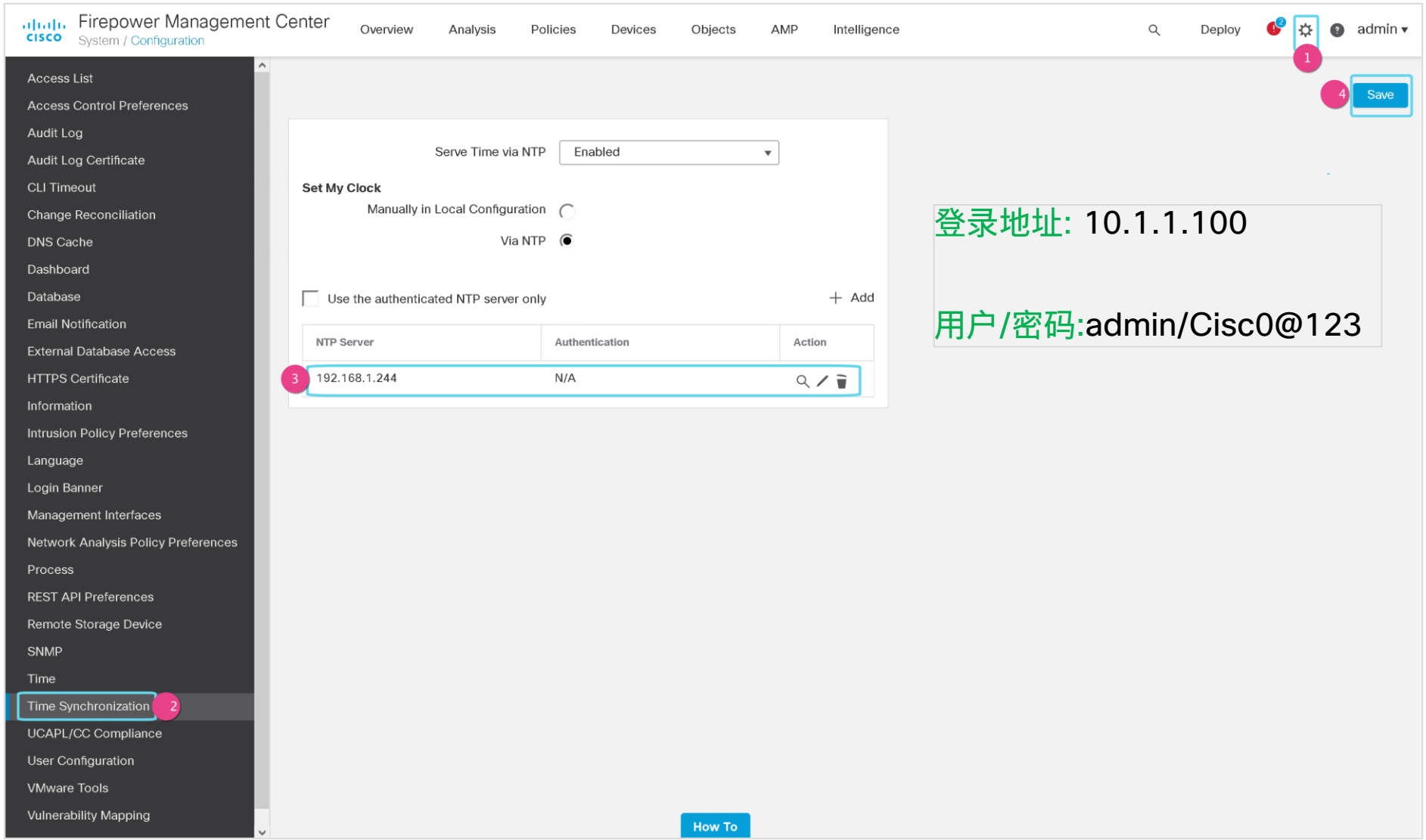


激活WIN2008 NTP

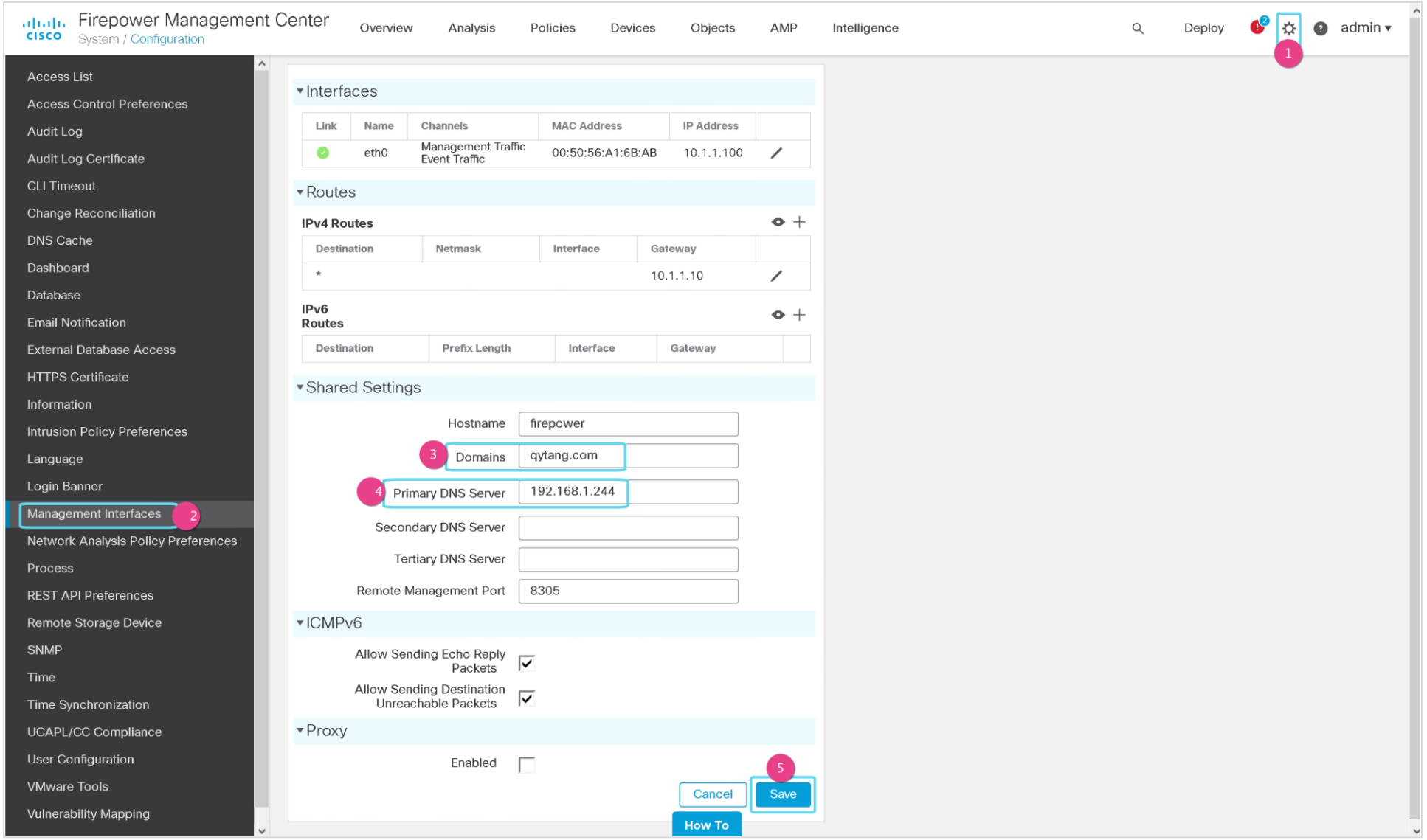




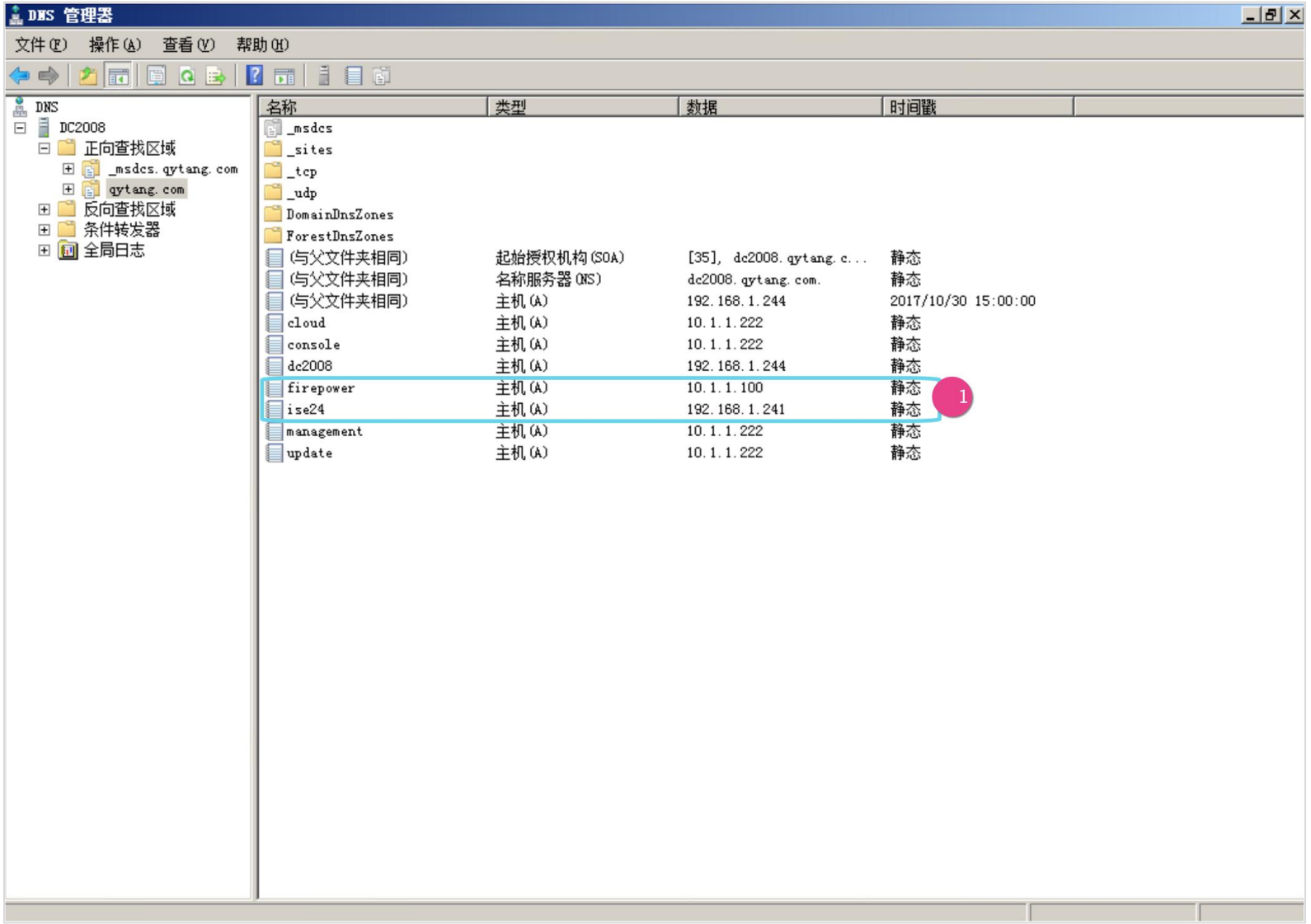
FMC配置NTP



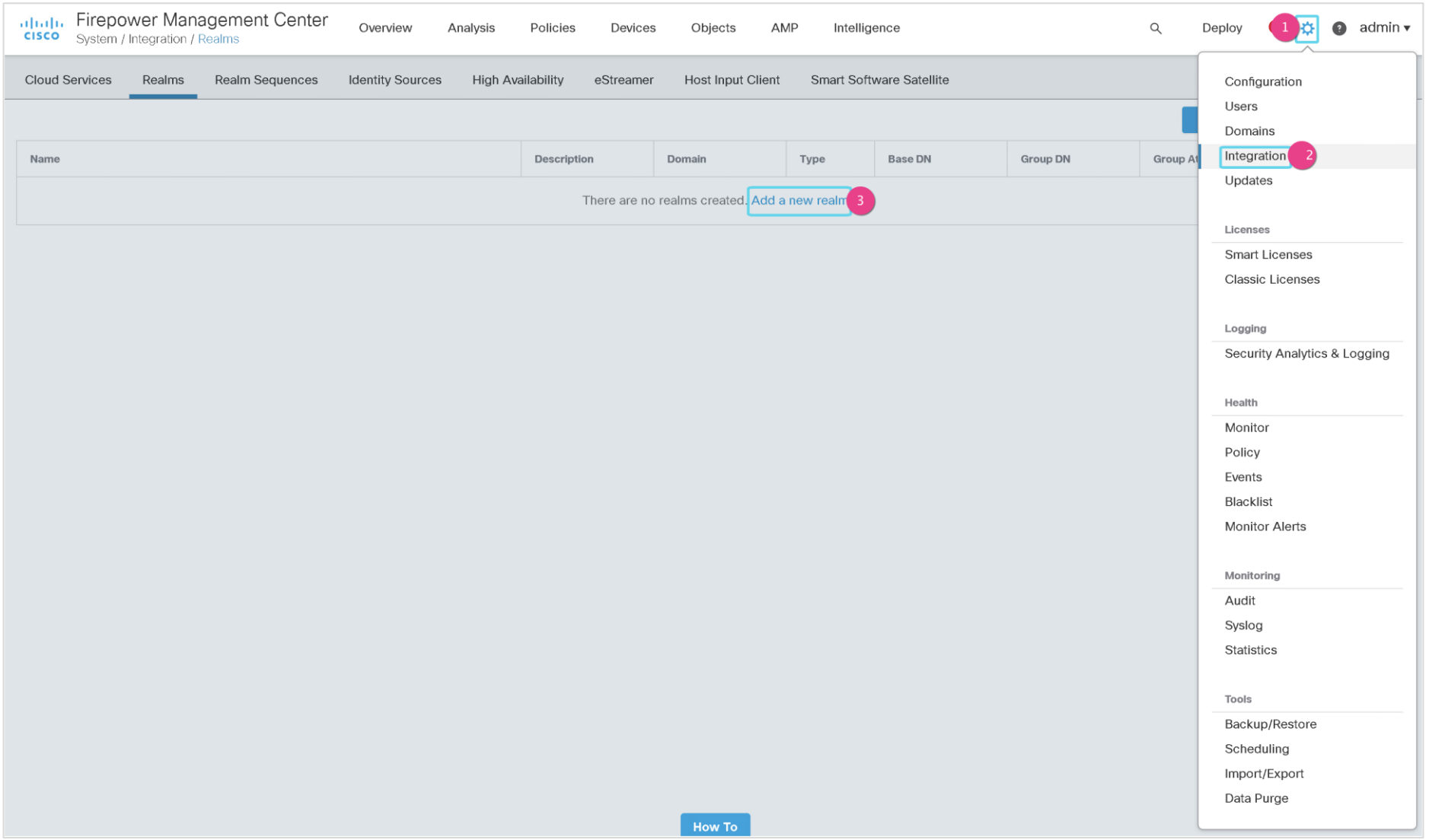
FMC配置DNS



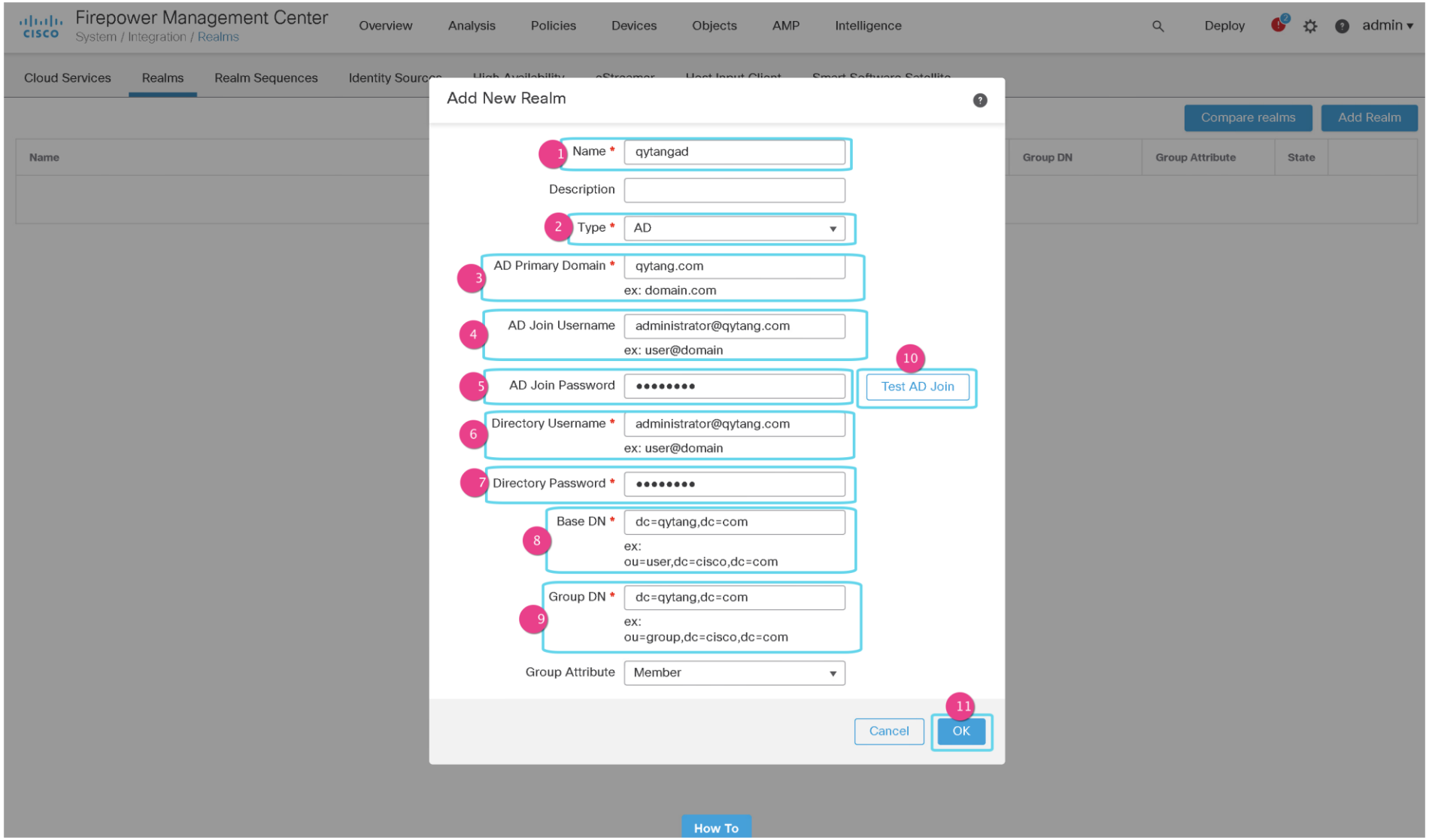
WIN2008 DNS配置



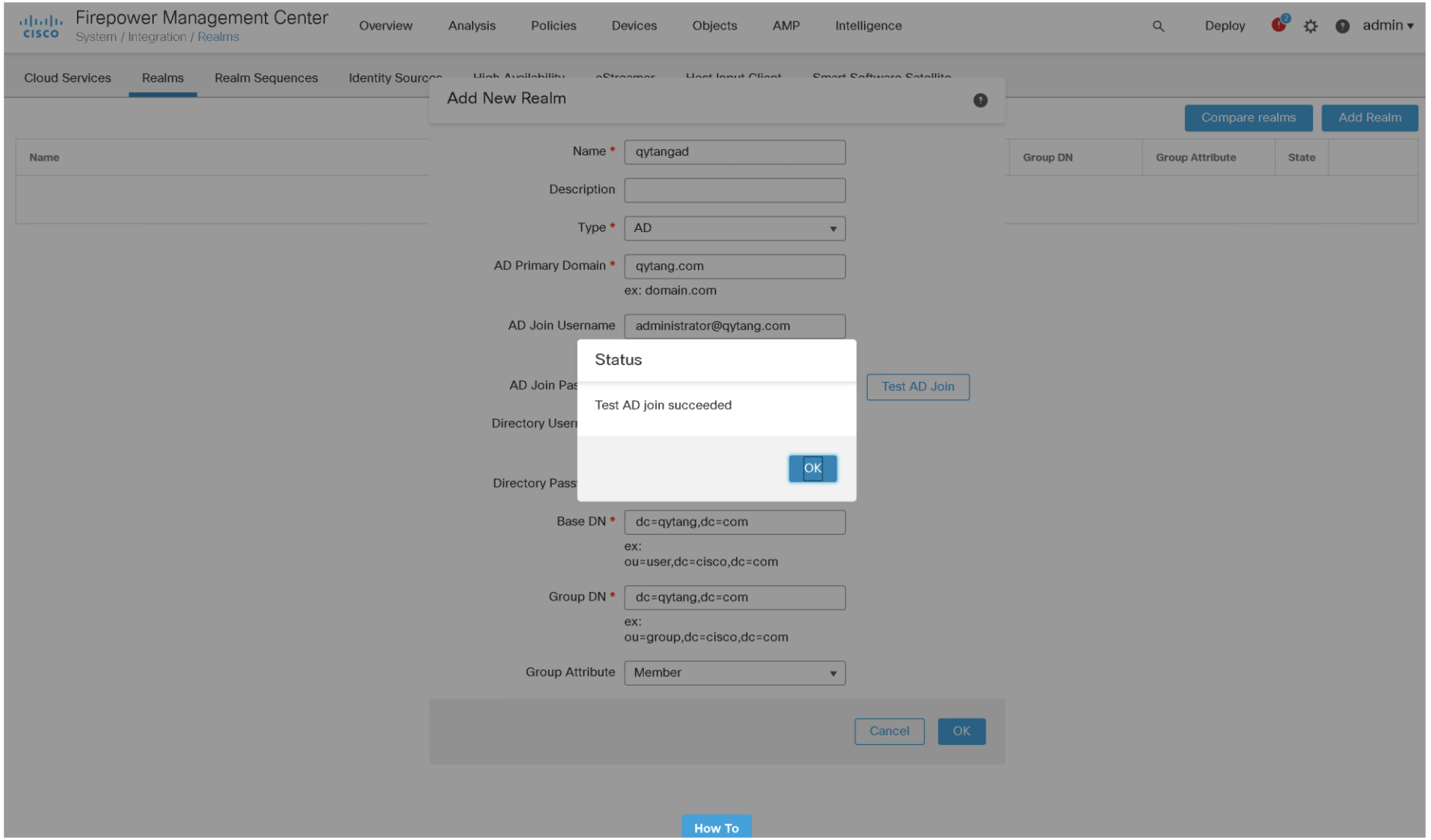
FMC整合AD(创建Realm)



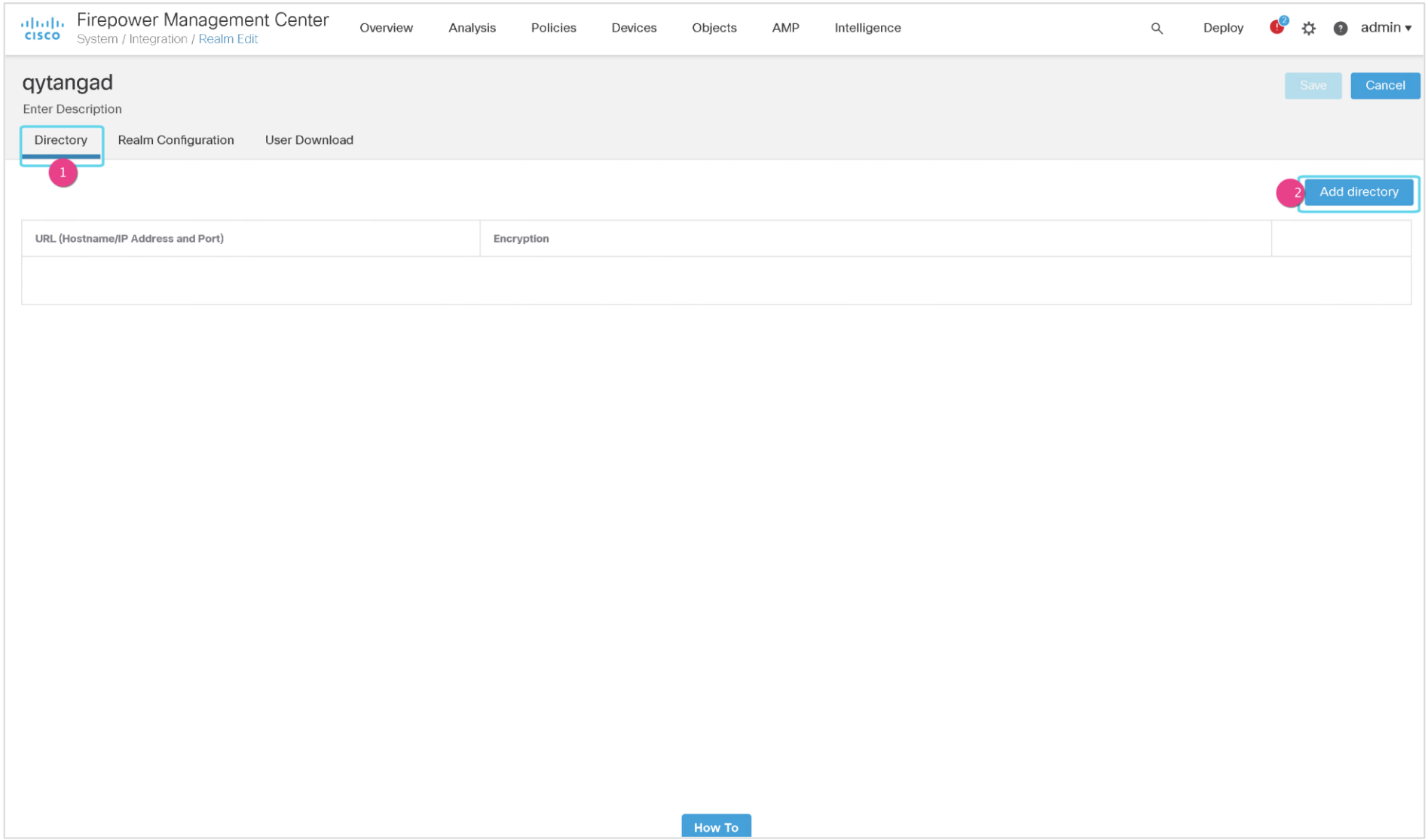
FMC整合AD(创建Realm)



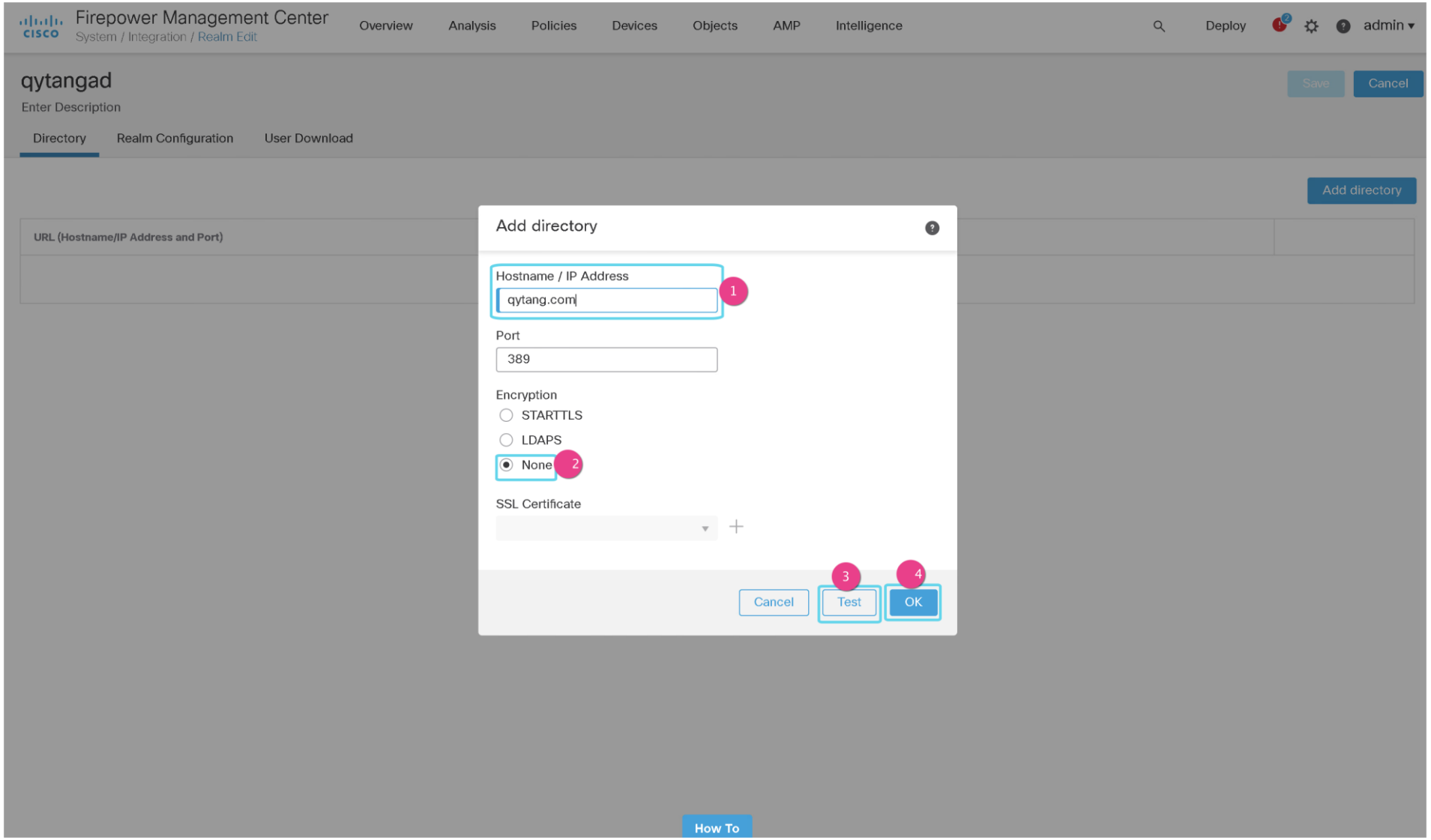
FMC整合AD(创建Realm)



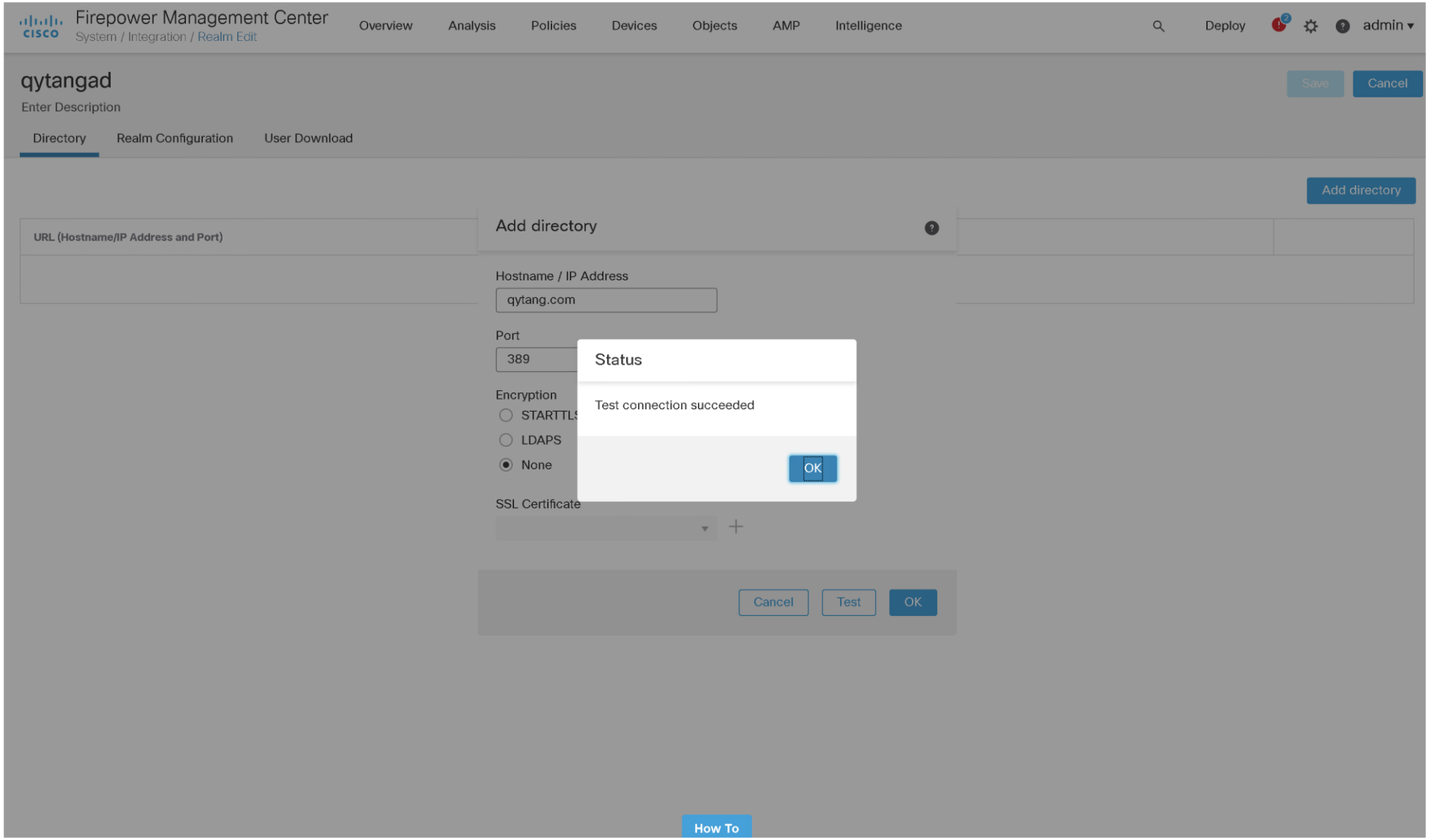
FMC整合AD(创建目录)



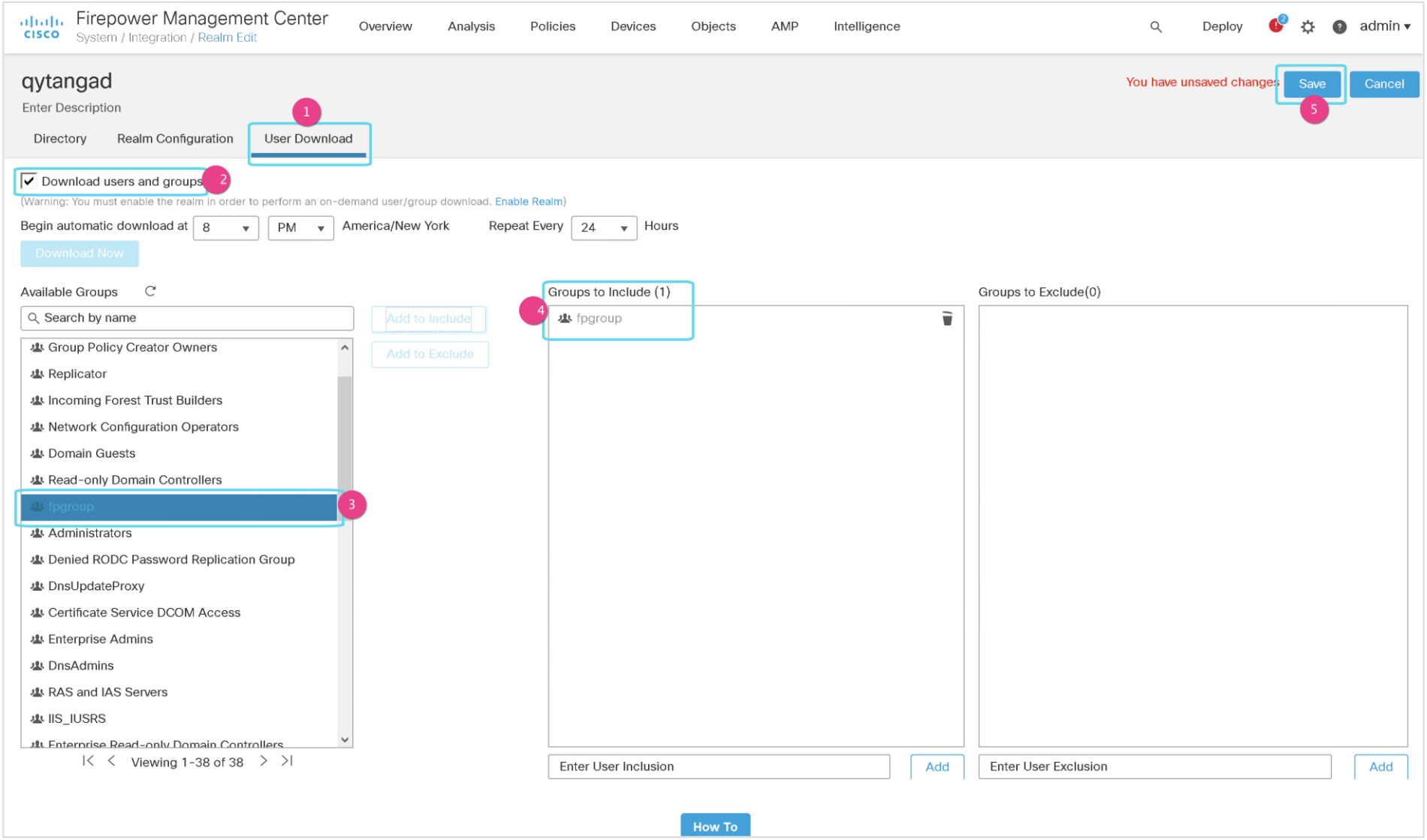
FMC整合AD(创建目录)



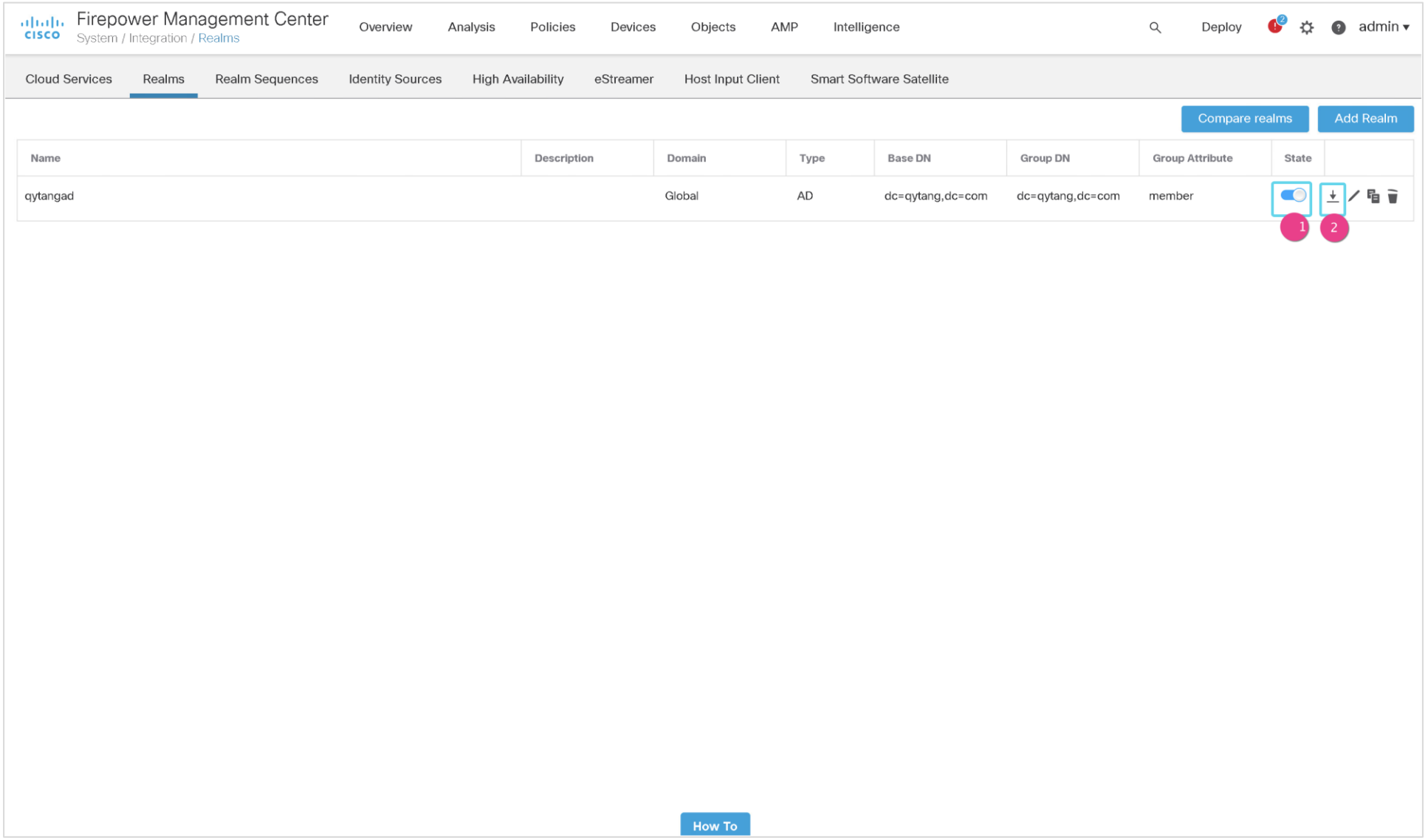
FMC整合AD(创建目录)



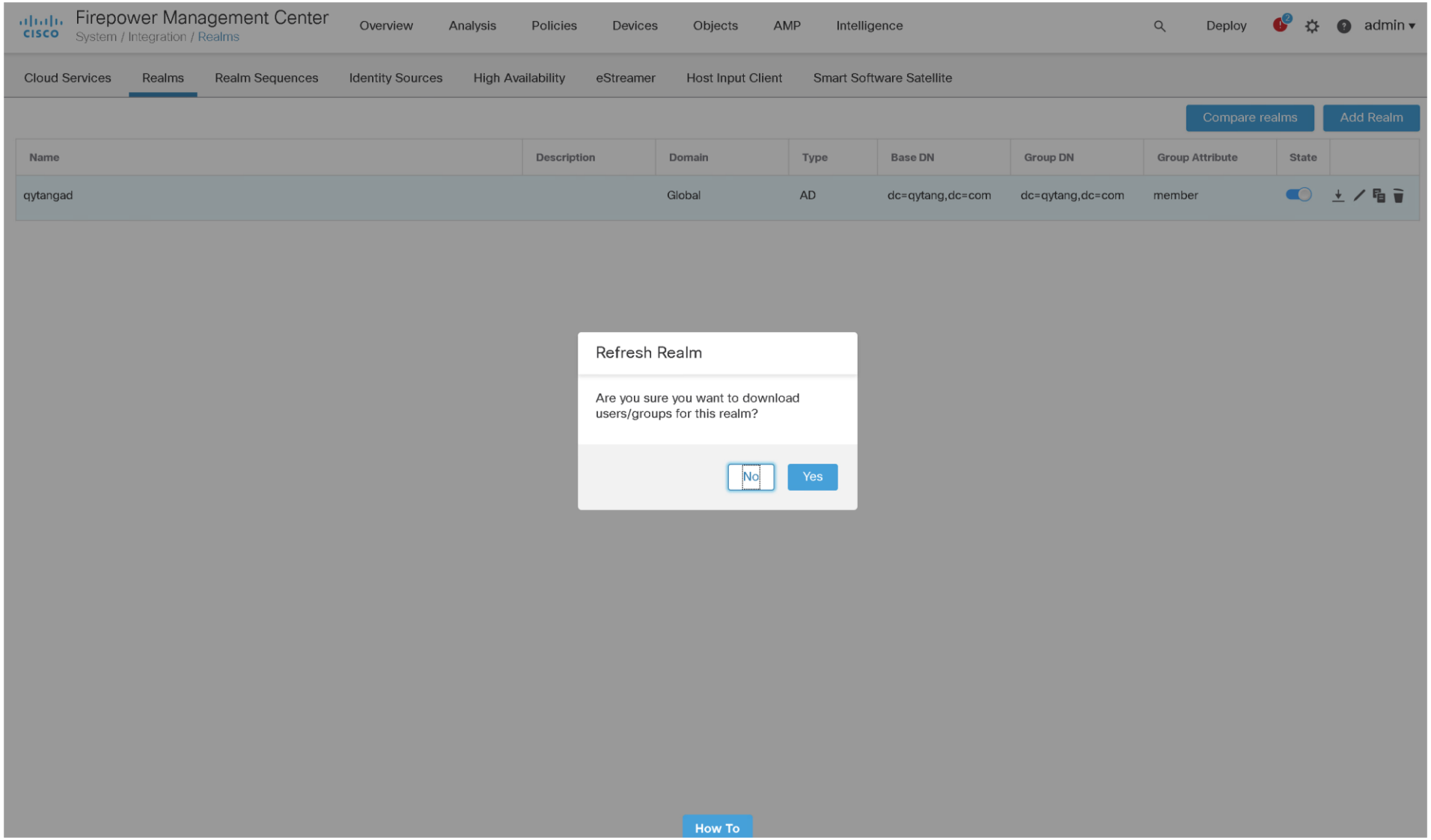
FMC整合AD(选择组)



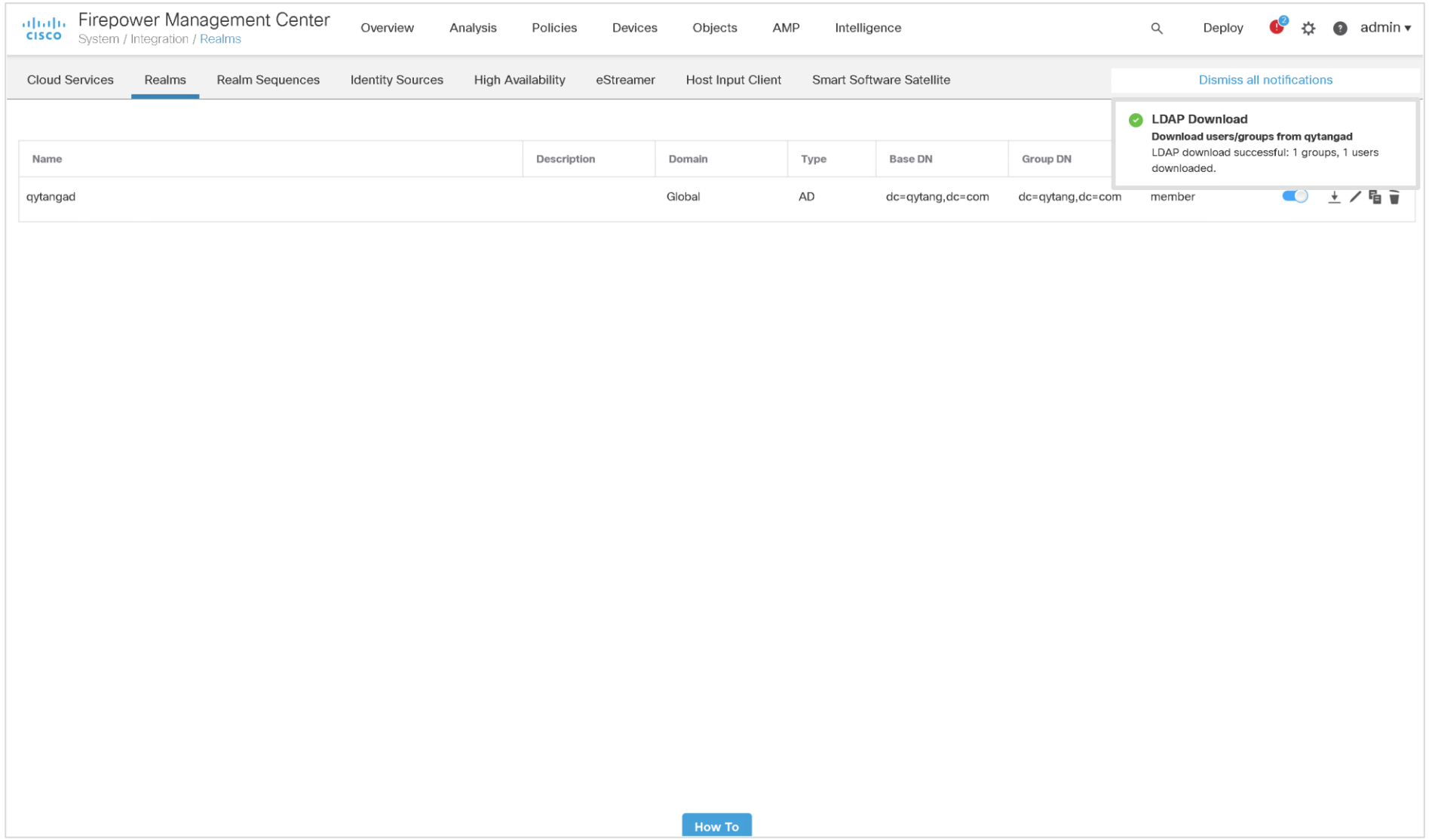
FMC整合AD(下载用户和组)



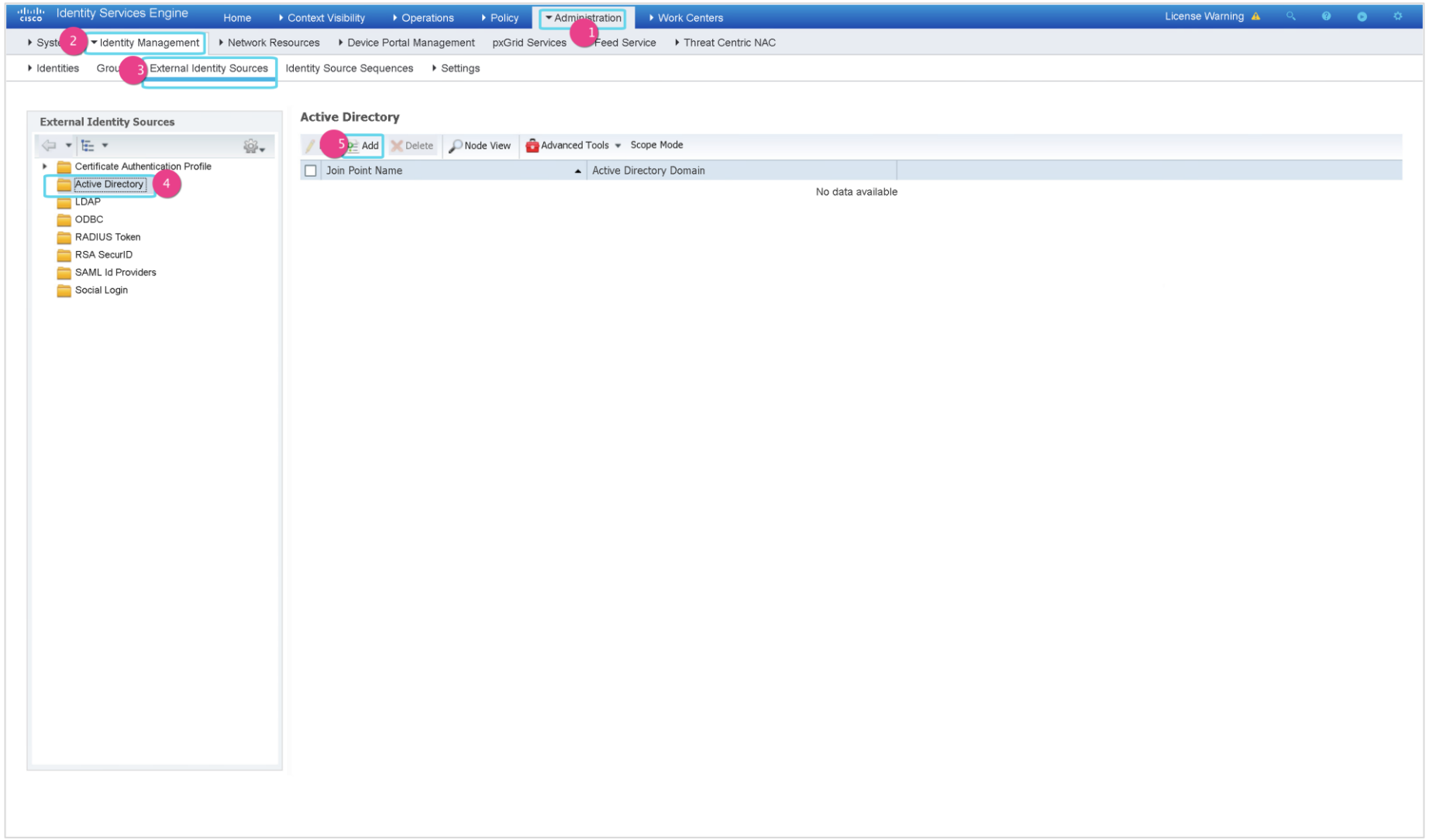
FMC整合AD(下载用户和组)



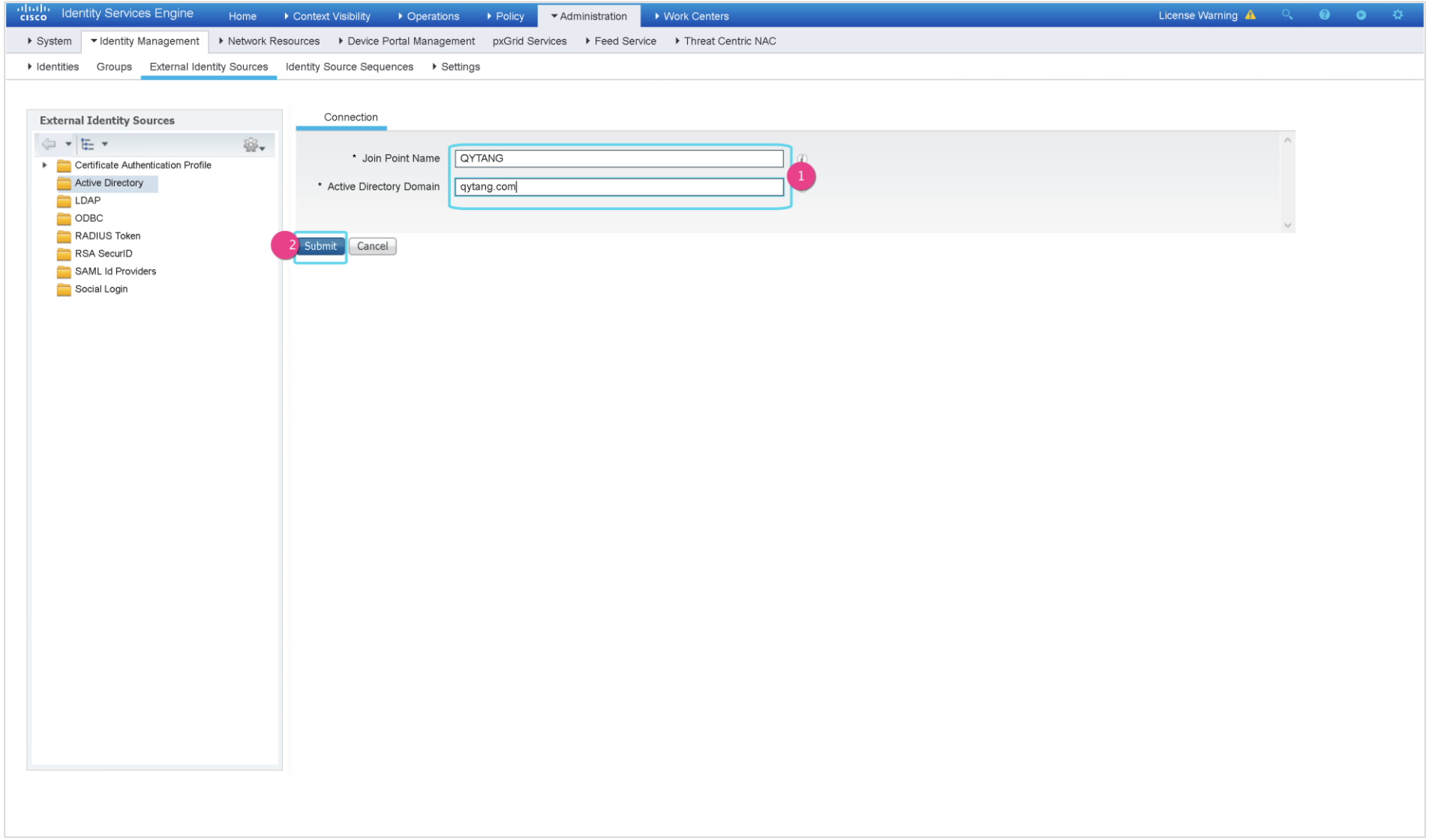
FMC整合AD(下载用户和组)



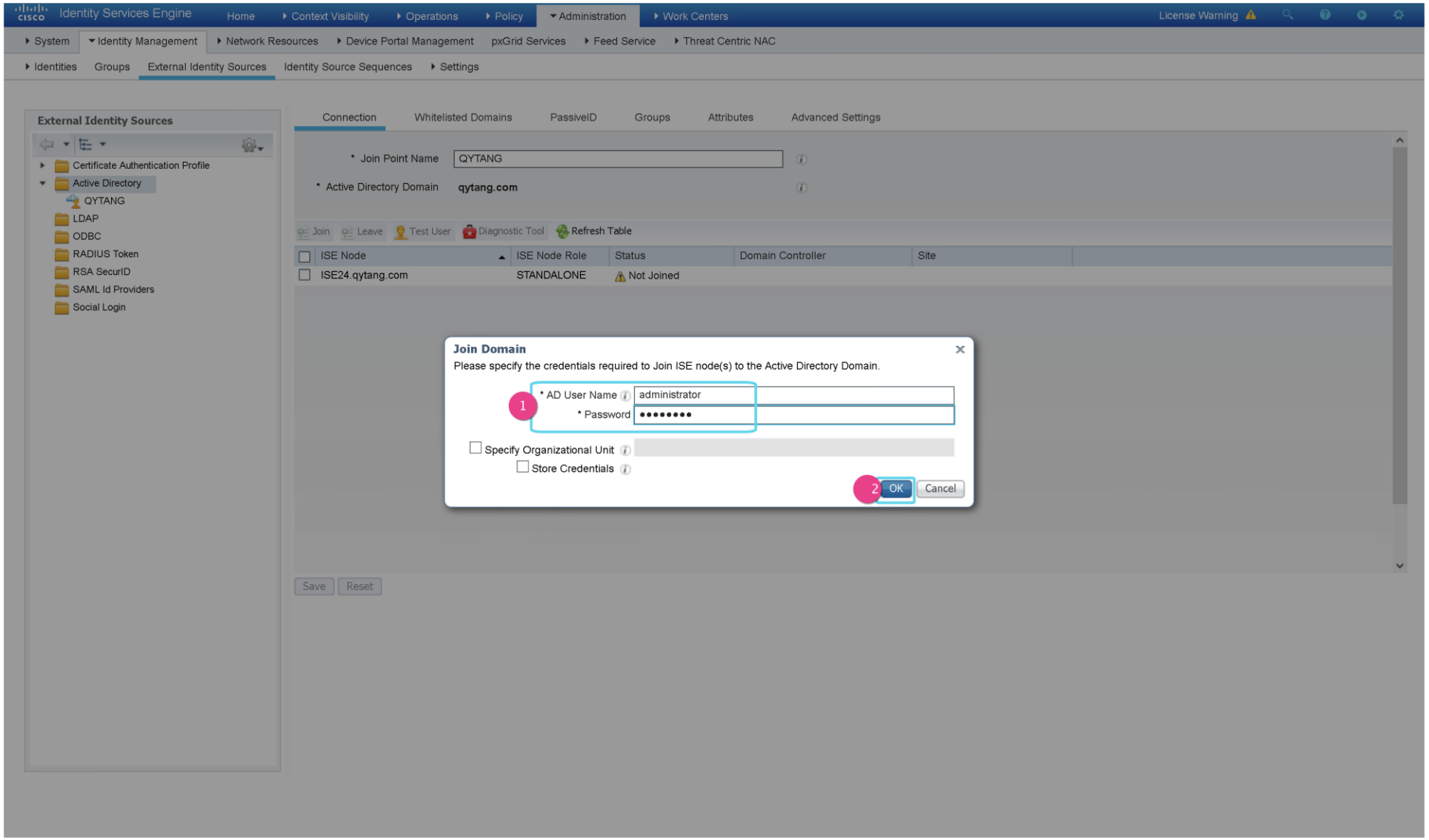
ISE整合AD(添加域)



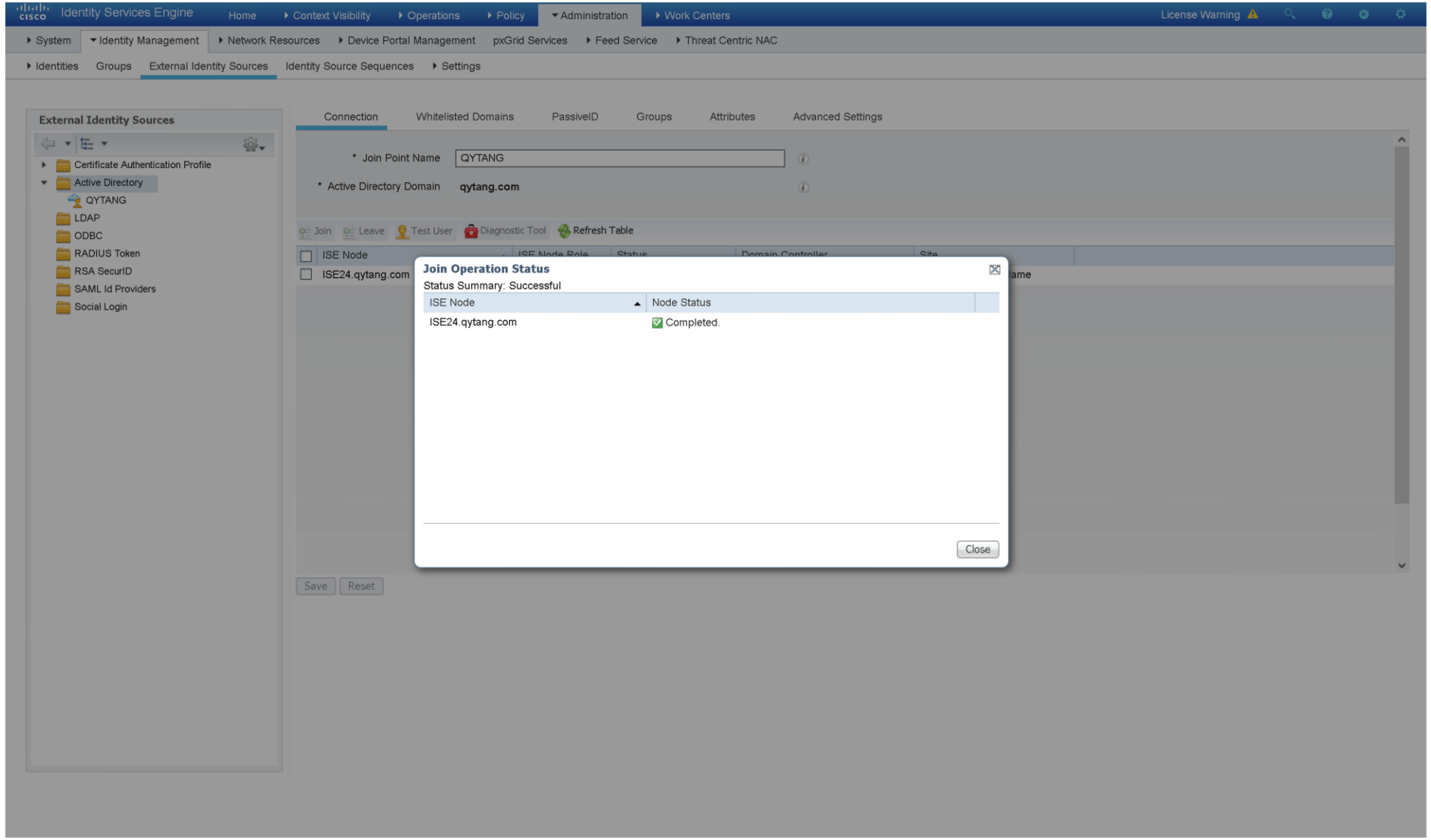
ISE整合AD(添加域)



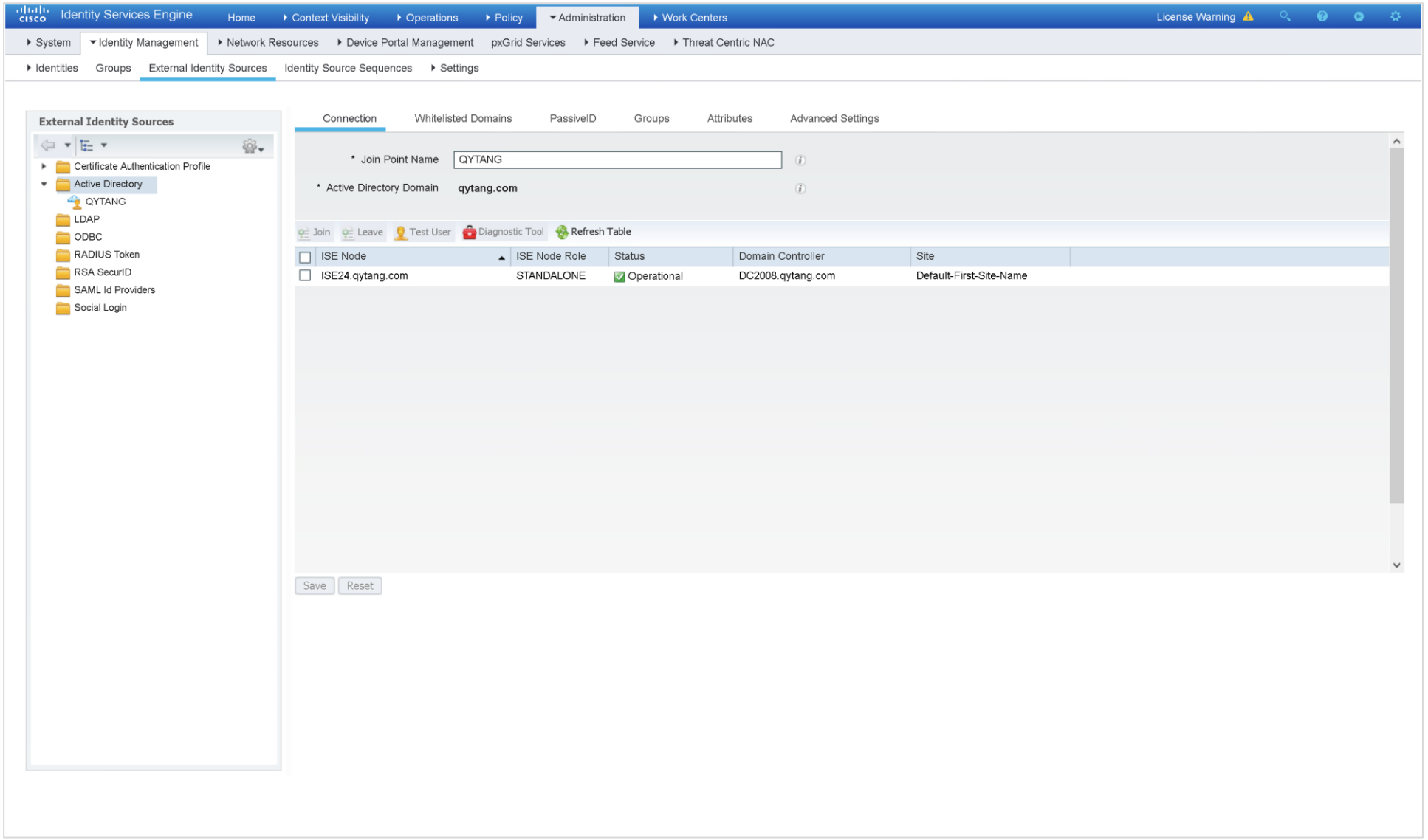
ISE整合AD(添加域)



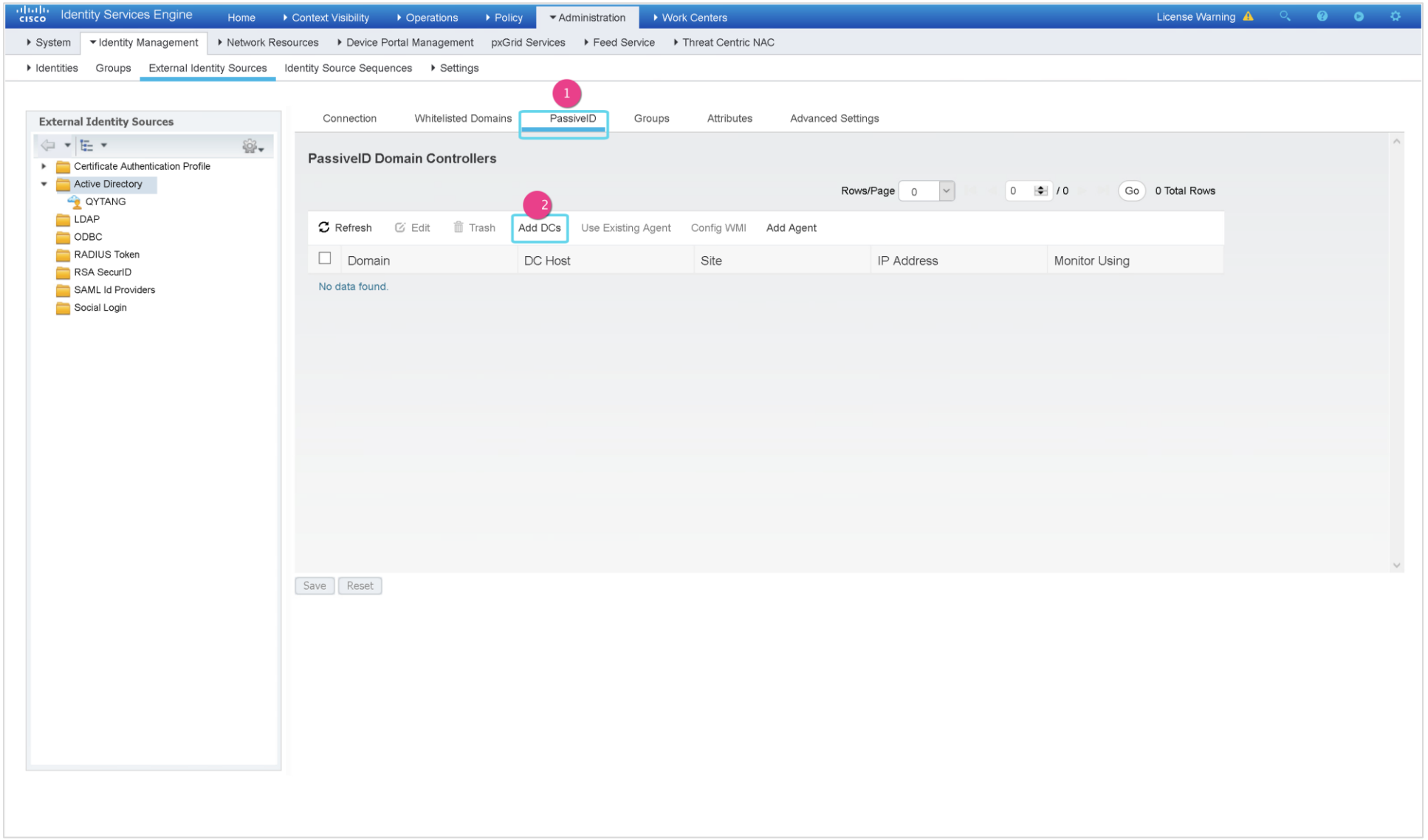
ISE整合AD(添加域)



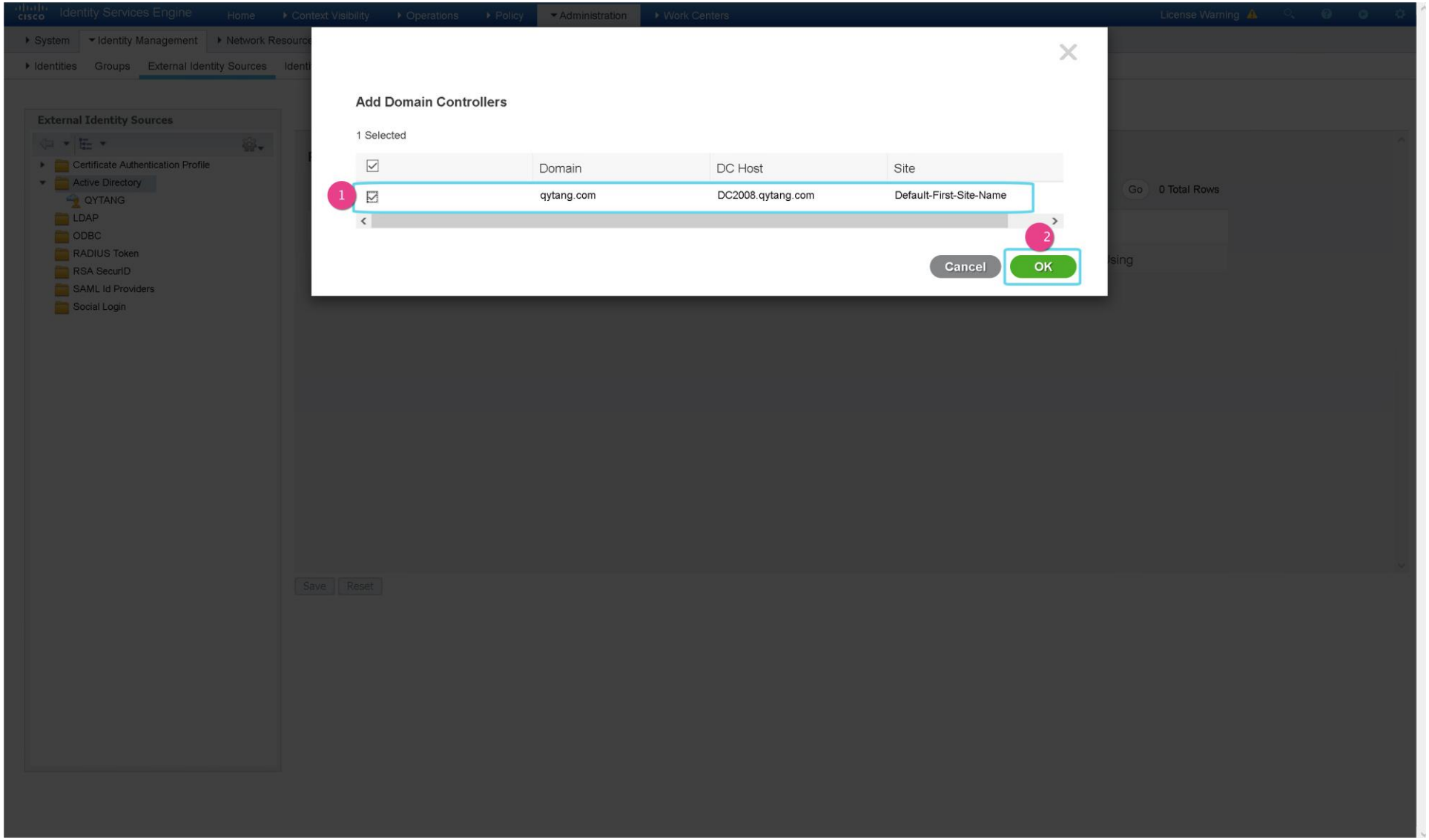
ISE整合AD(添加域)



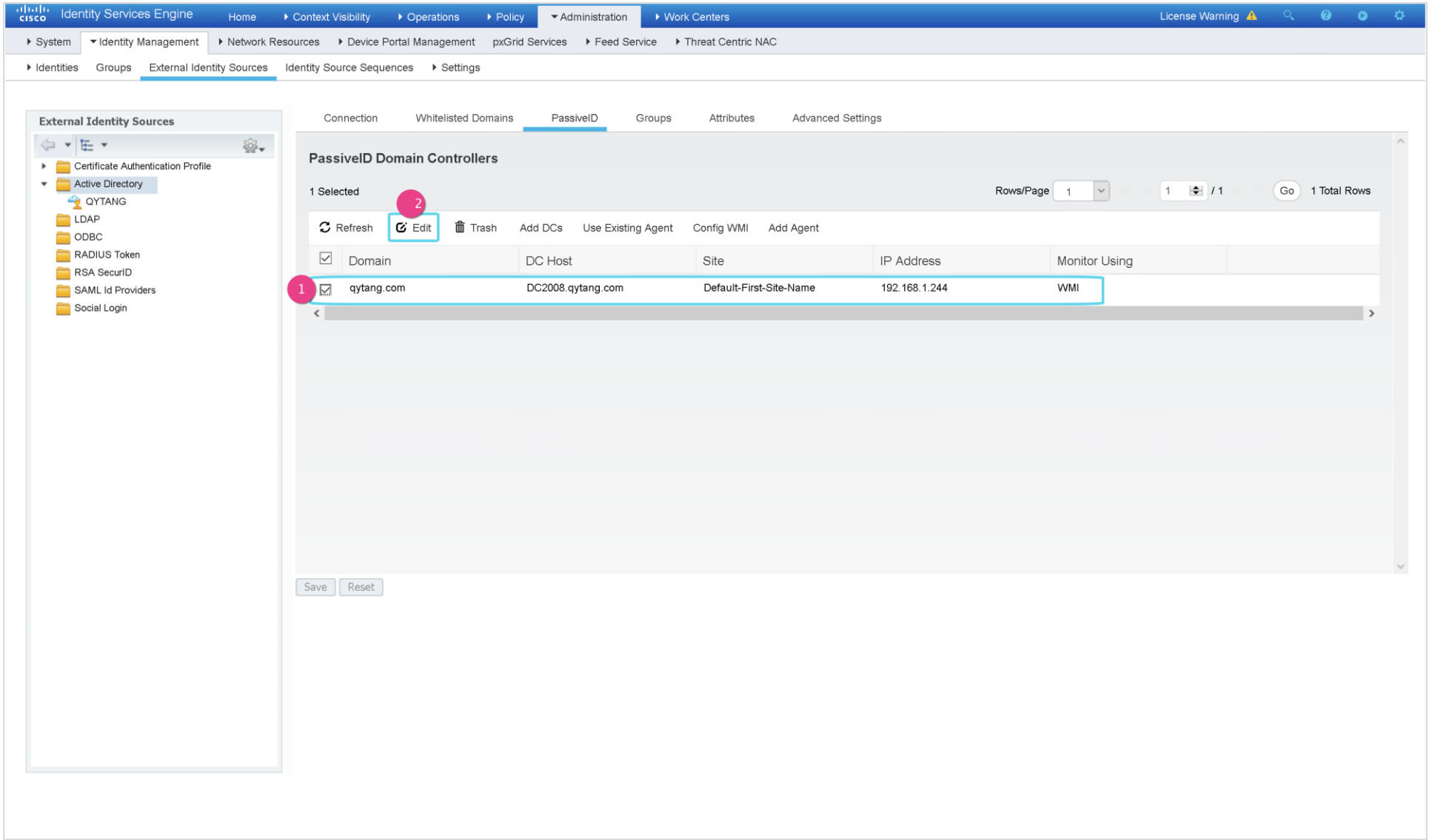
ISE整合AD(添加PassiveID)



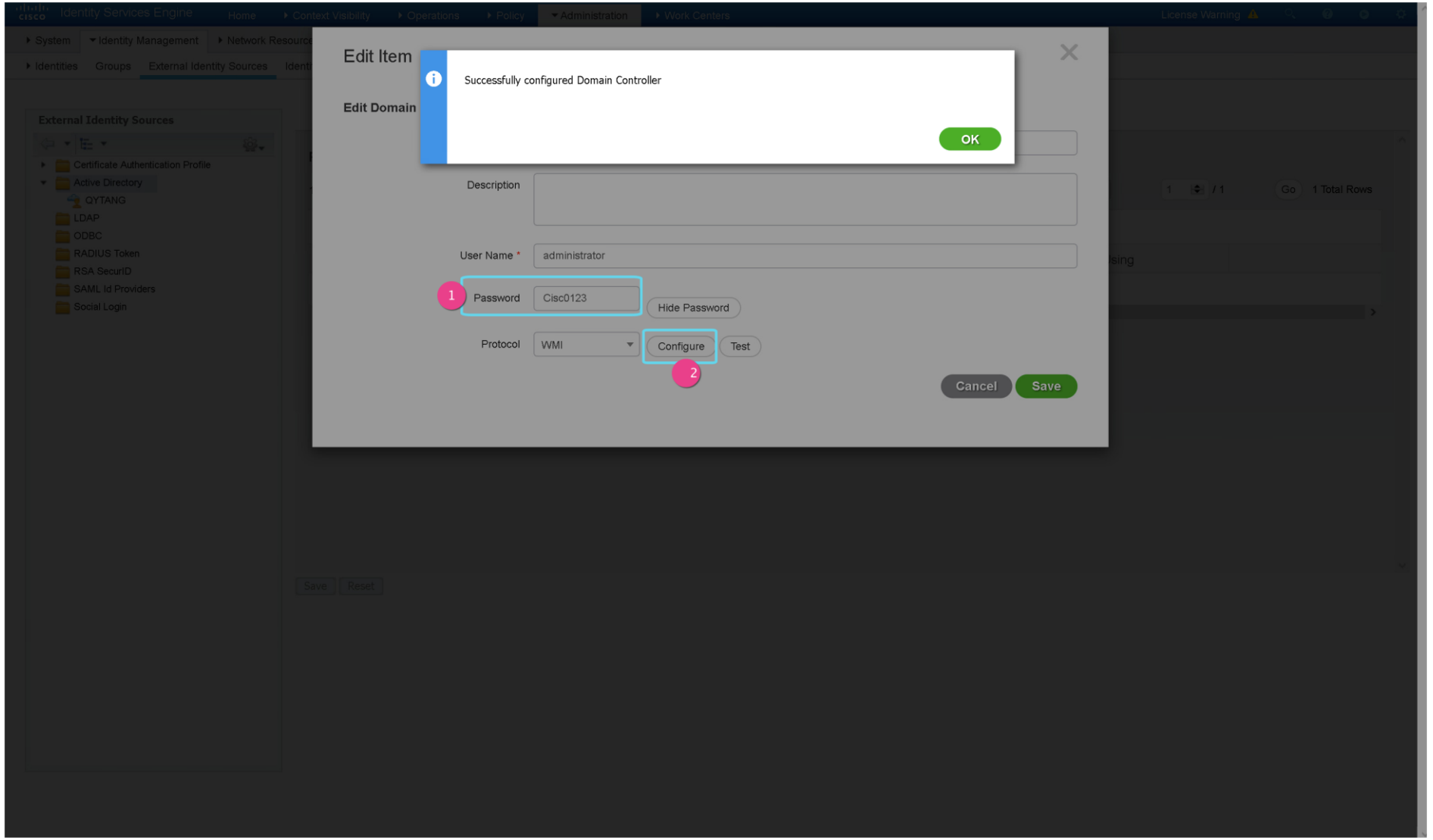
ISE整合AD(添加PassiveID)



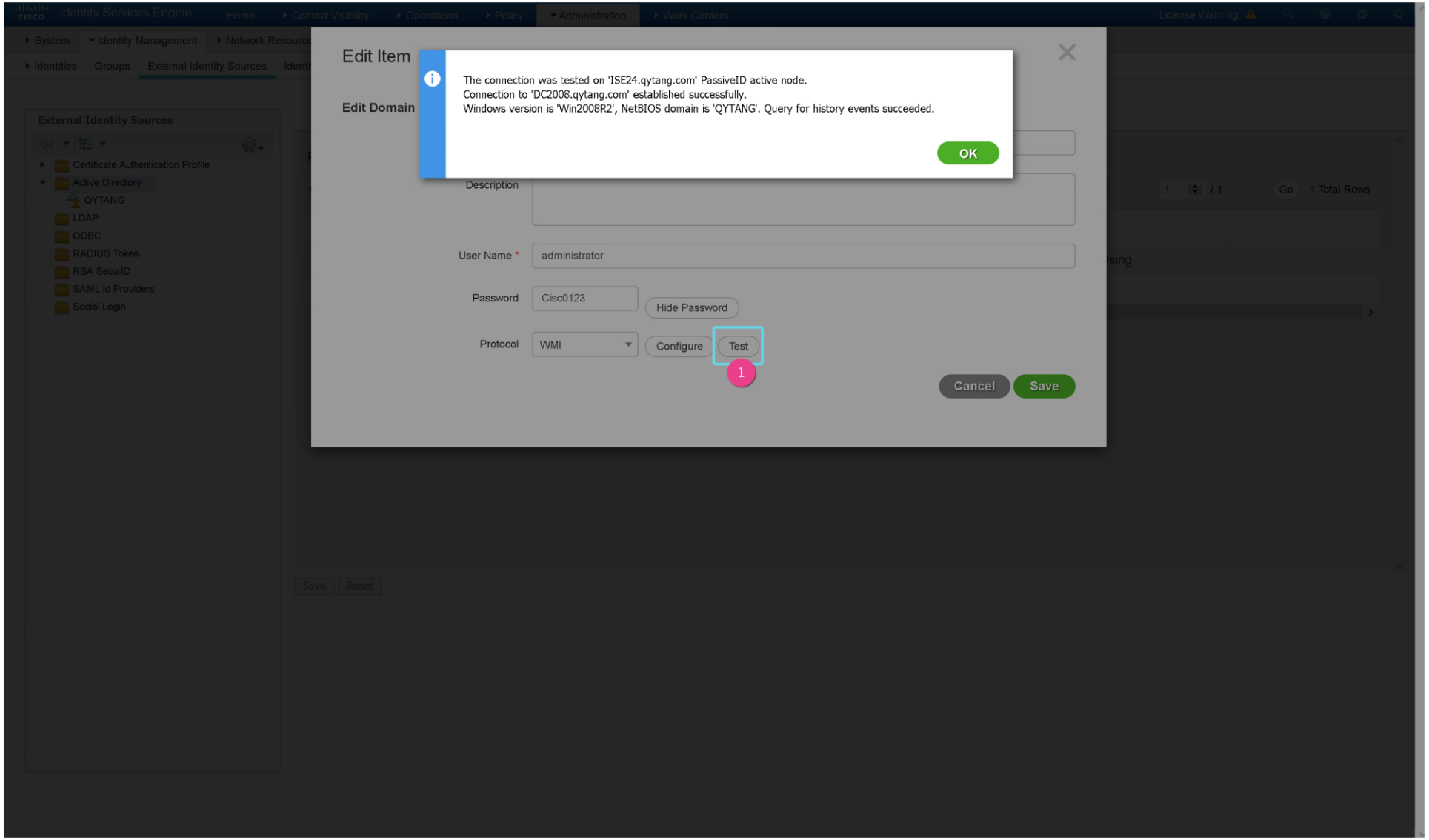
ISE整合AD(添加PassiveID)



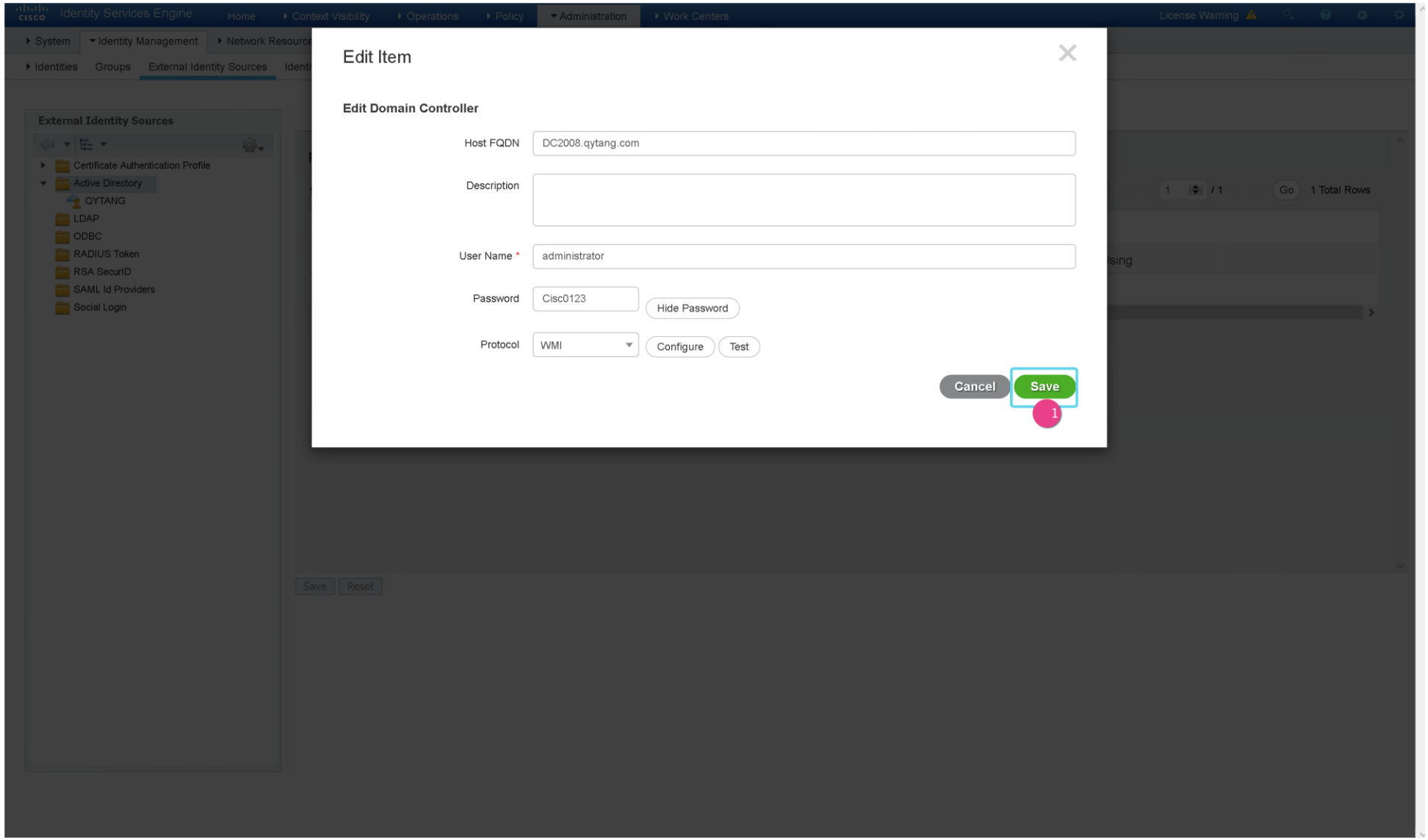
ISE整合AD(添加PassiveID)



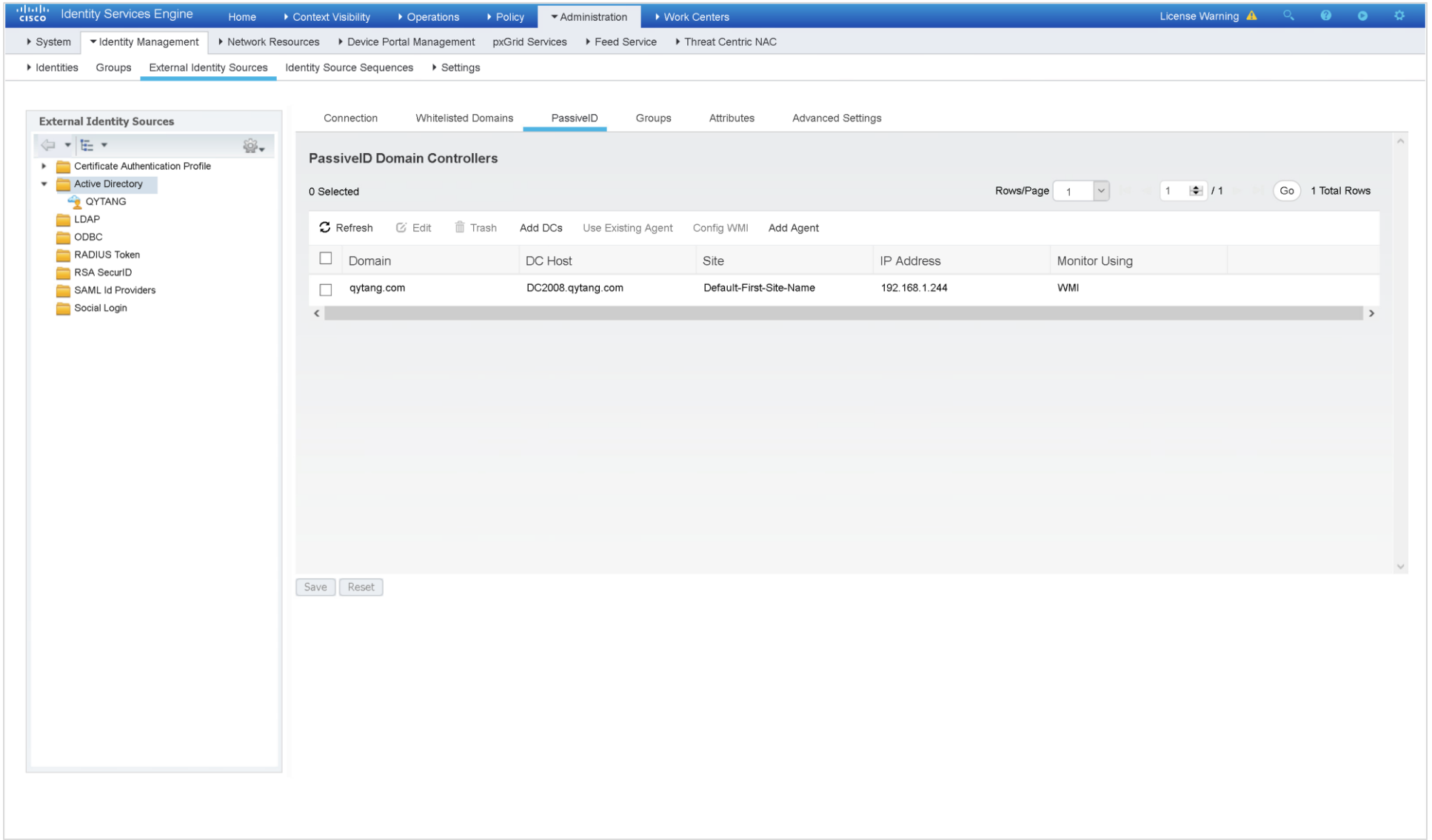
ISE整合AD(添加PassiveID)



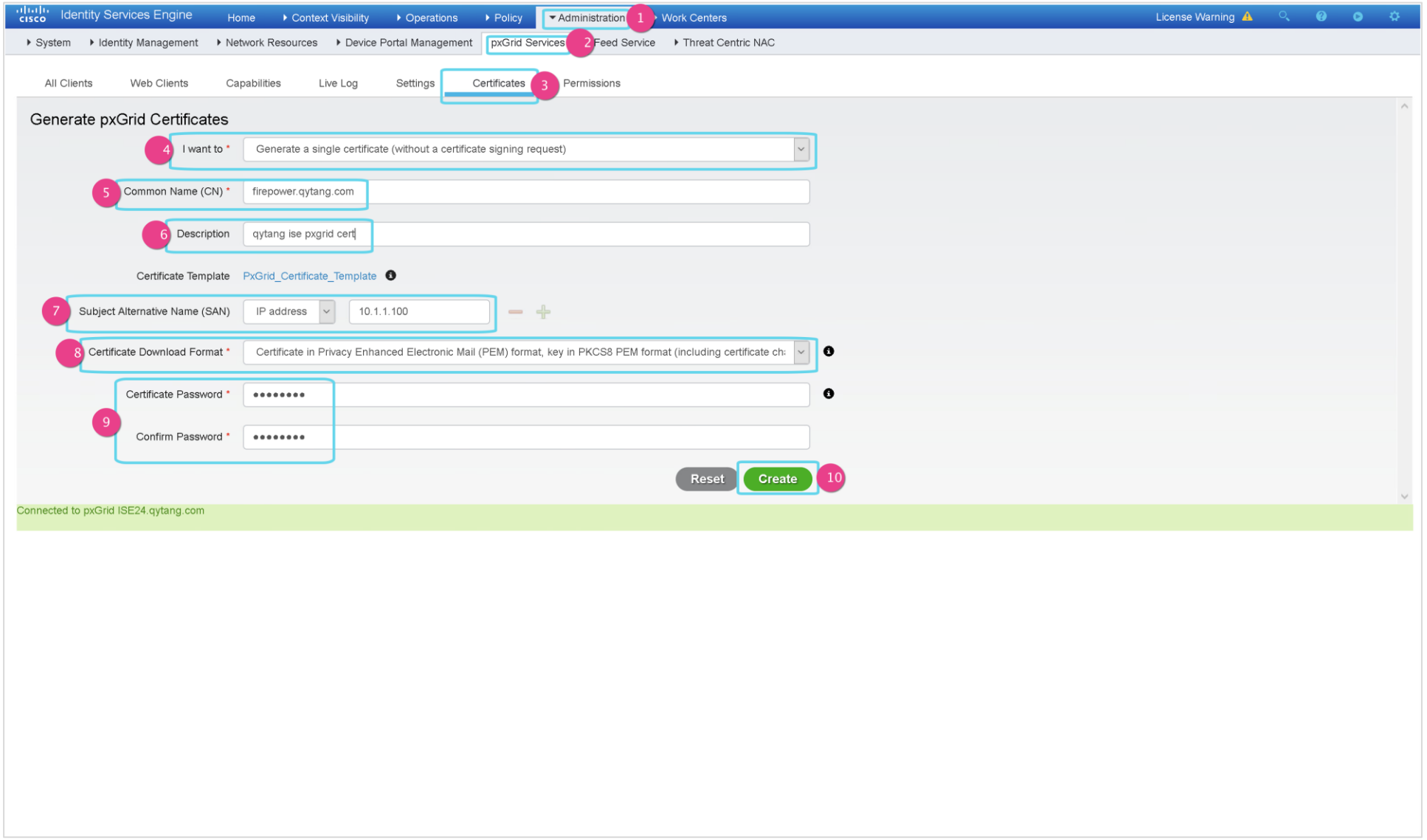
ISE整合AD(添加PassiveID)



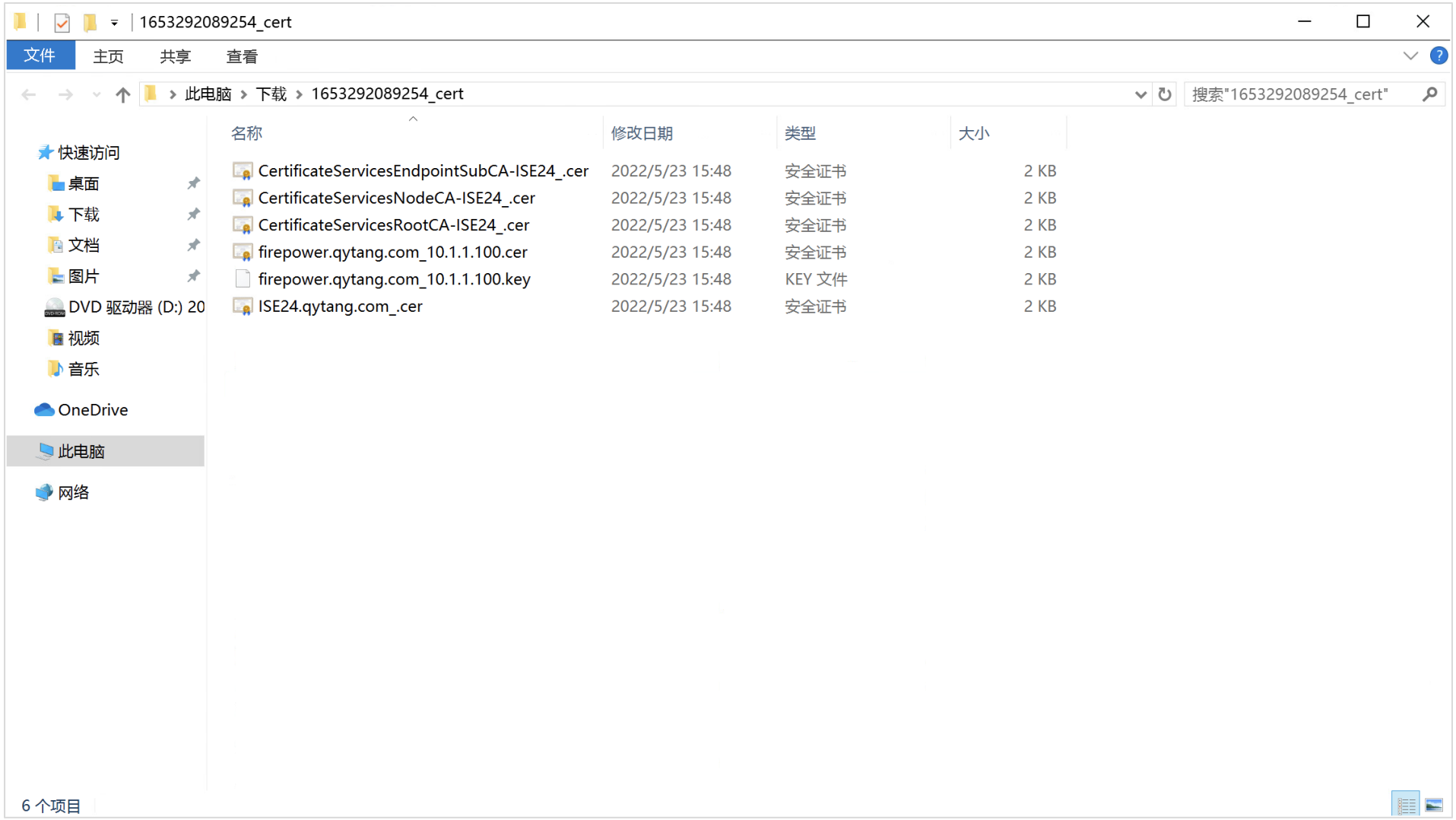
ISE整合AD(添加PassiveID)



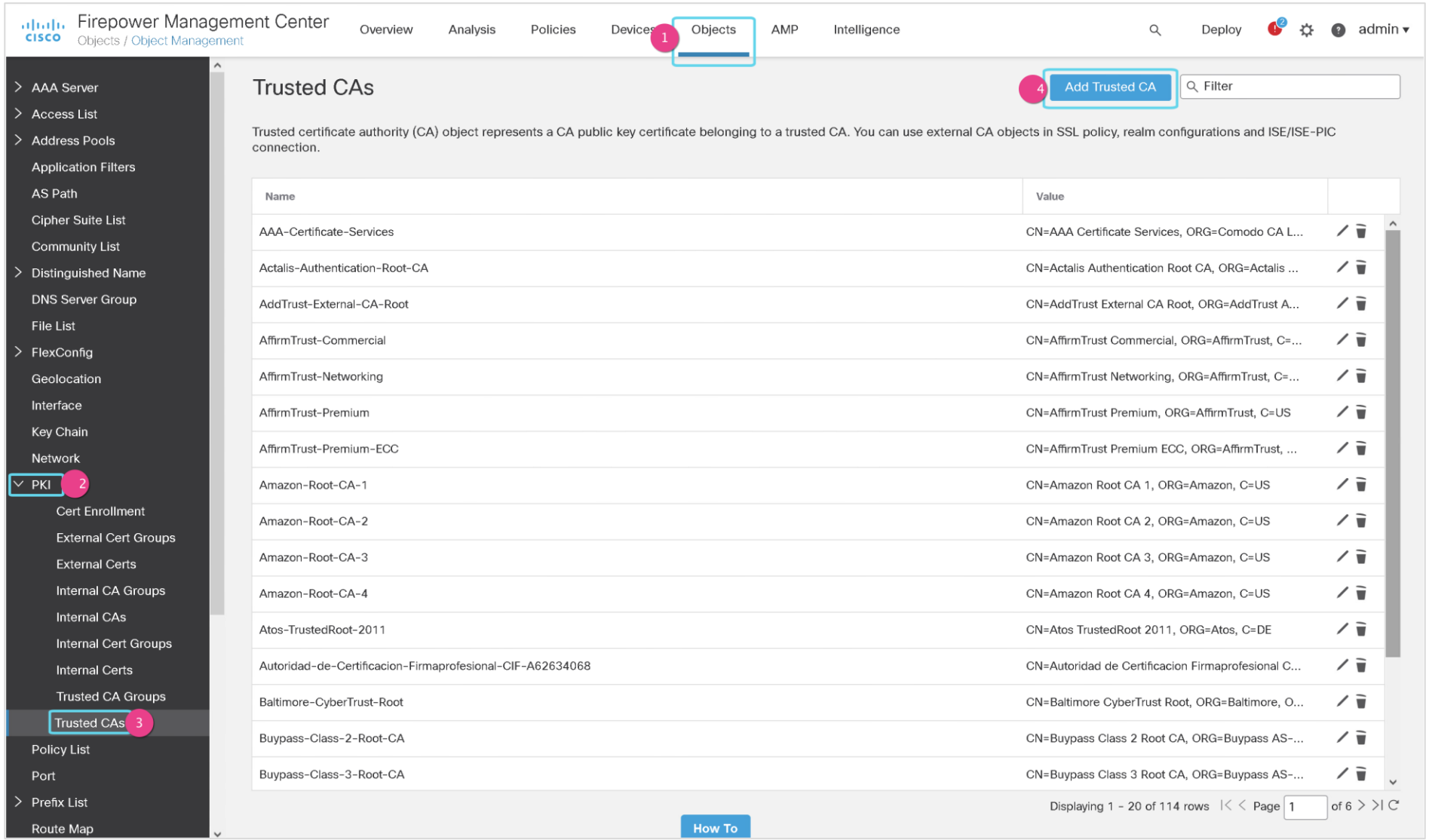
FMC与ISE之间的PxGrid(证书)



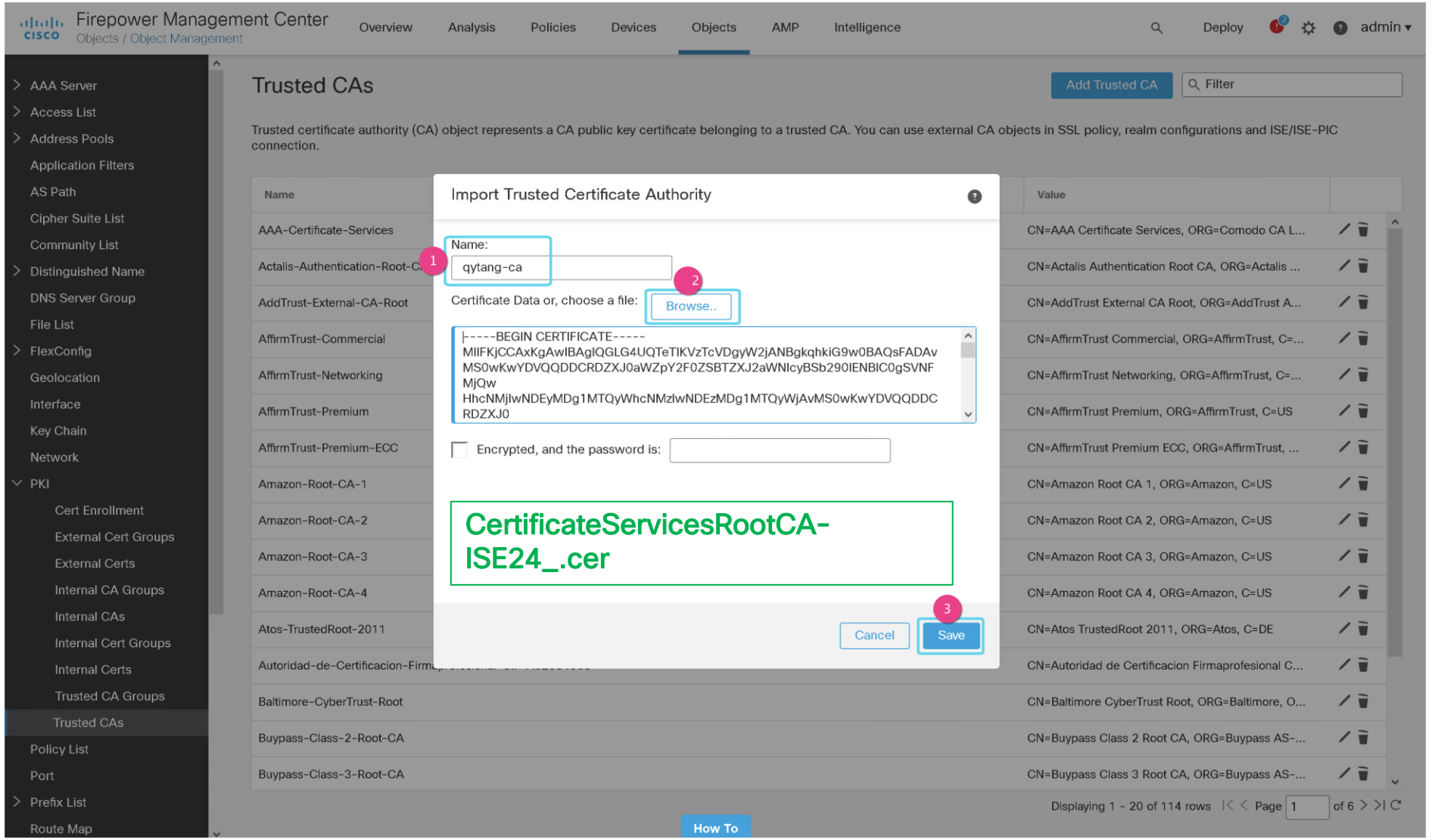
FMC与ISE之间的PxGrid(证书)



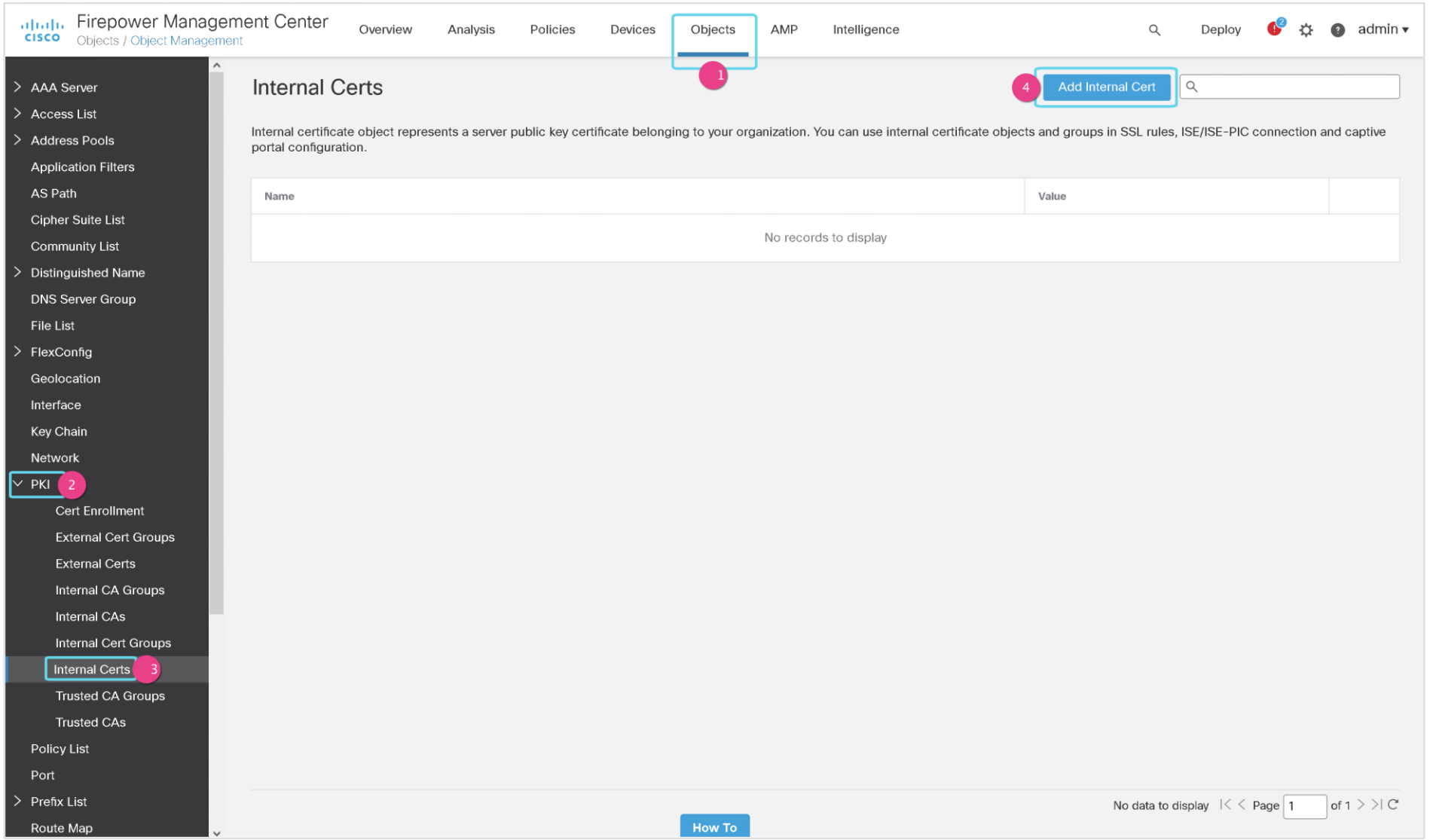
FMC与ISE之间的PxGrid(证书)



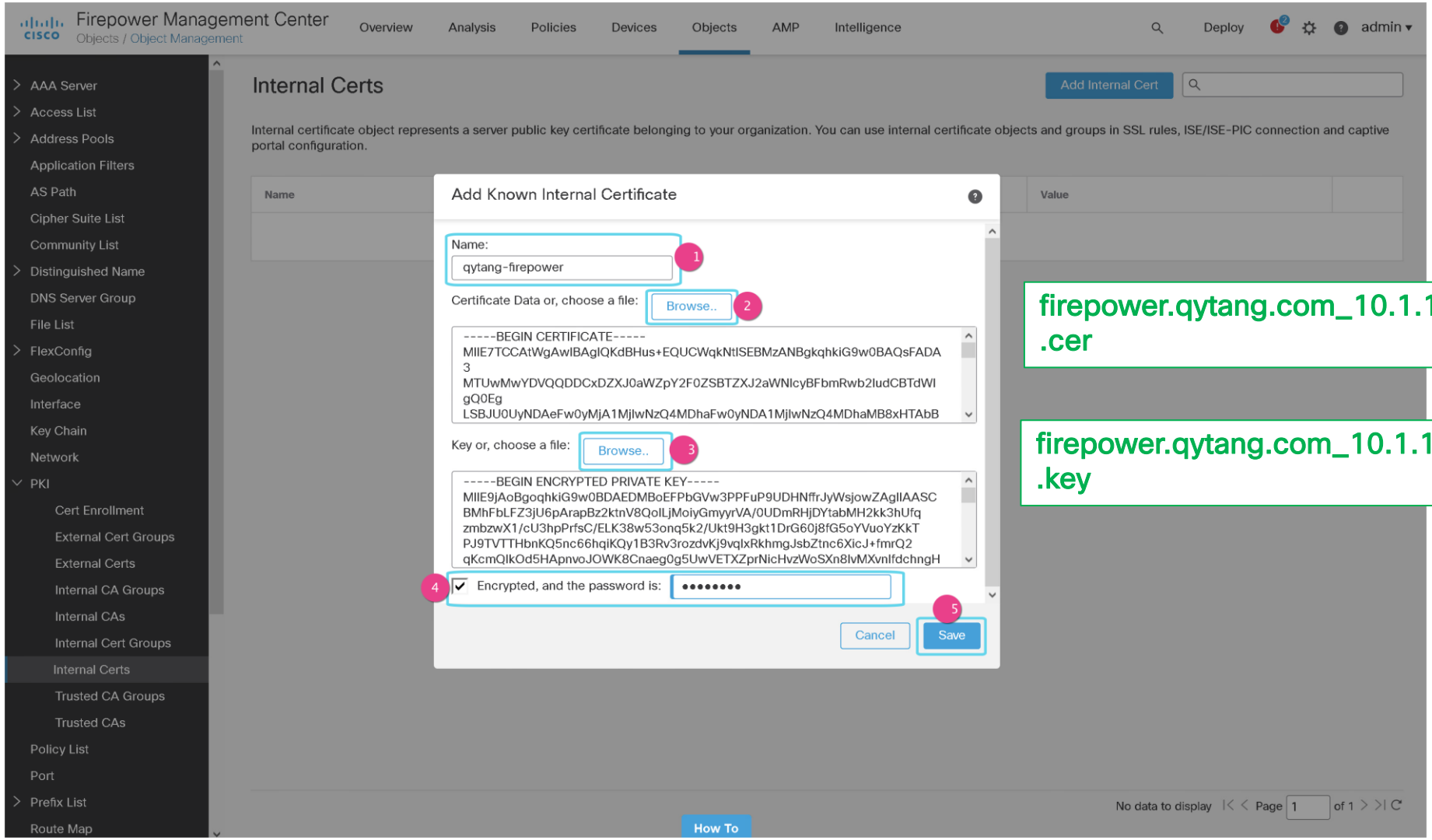
FMC与ISE之间的PxGrid(证书)



FMC与ISE之间的PxGrid(证书)



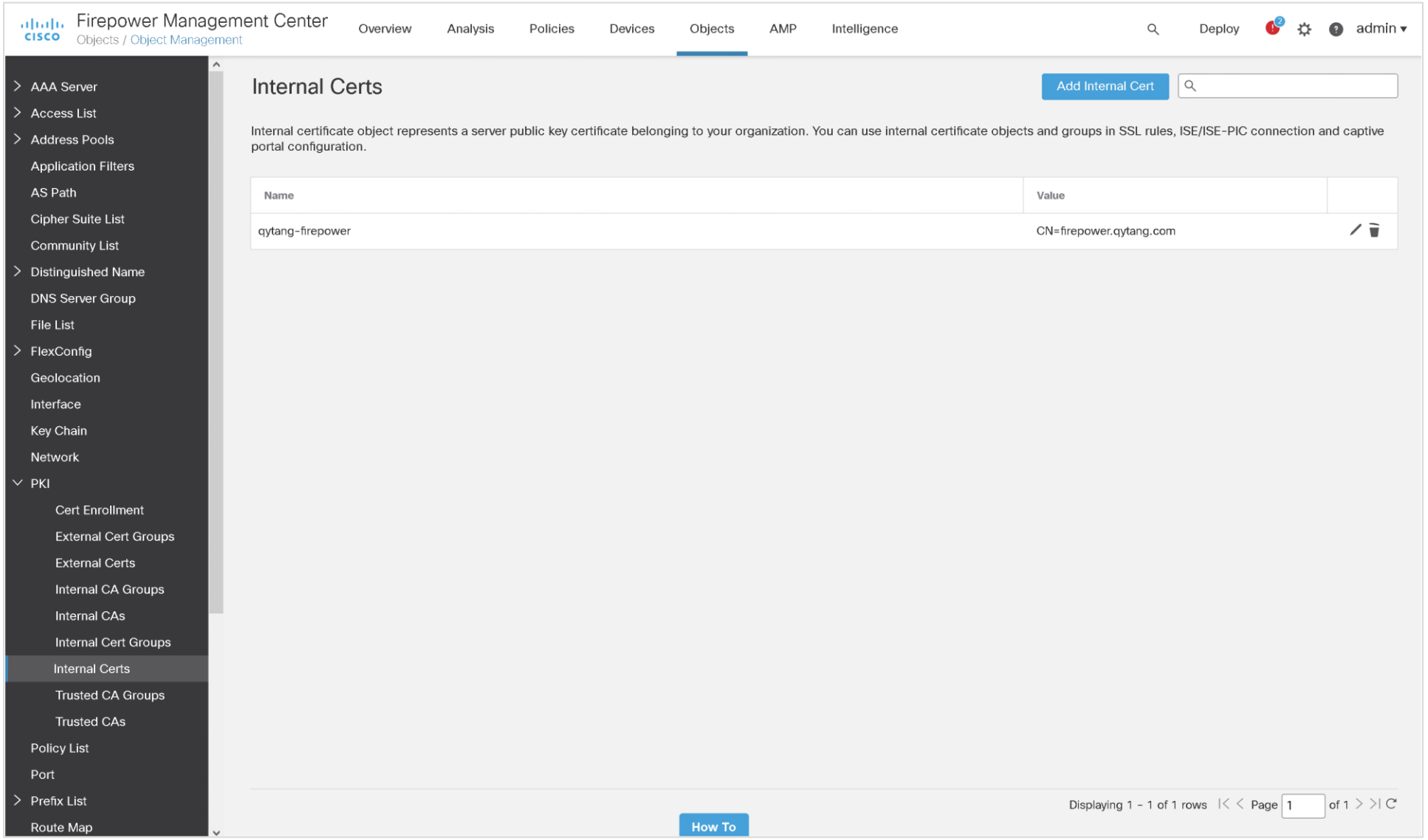
FMC与ISE之间的PxGrid(证书)



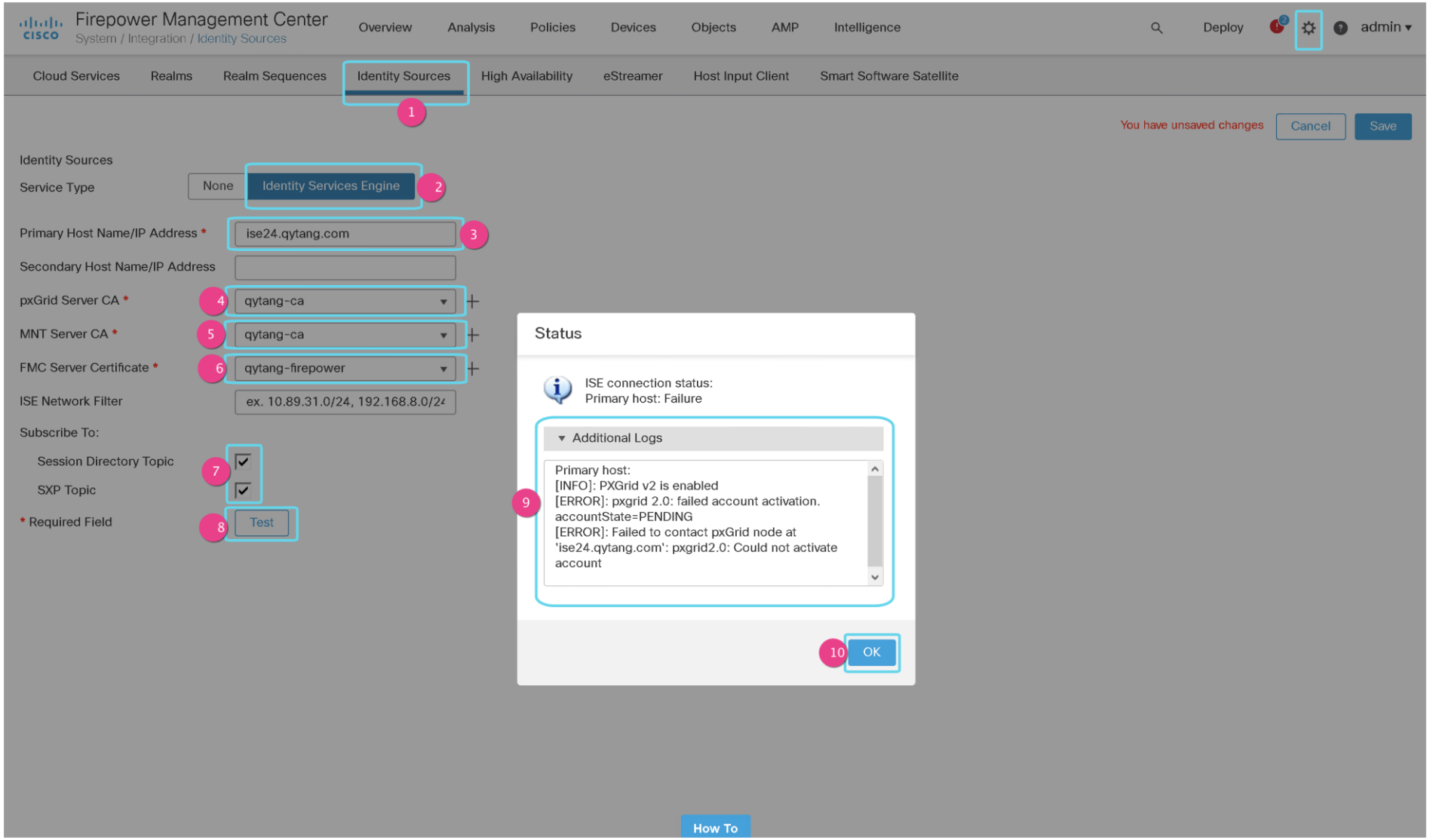
firepower.qytang.com_10.1.1.100.cer

firepower.qytang.com_10.1.1.100.key

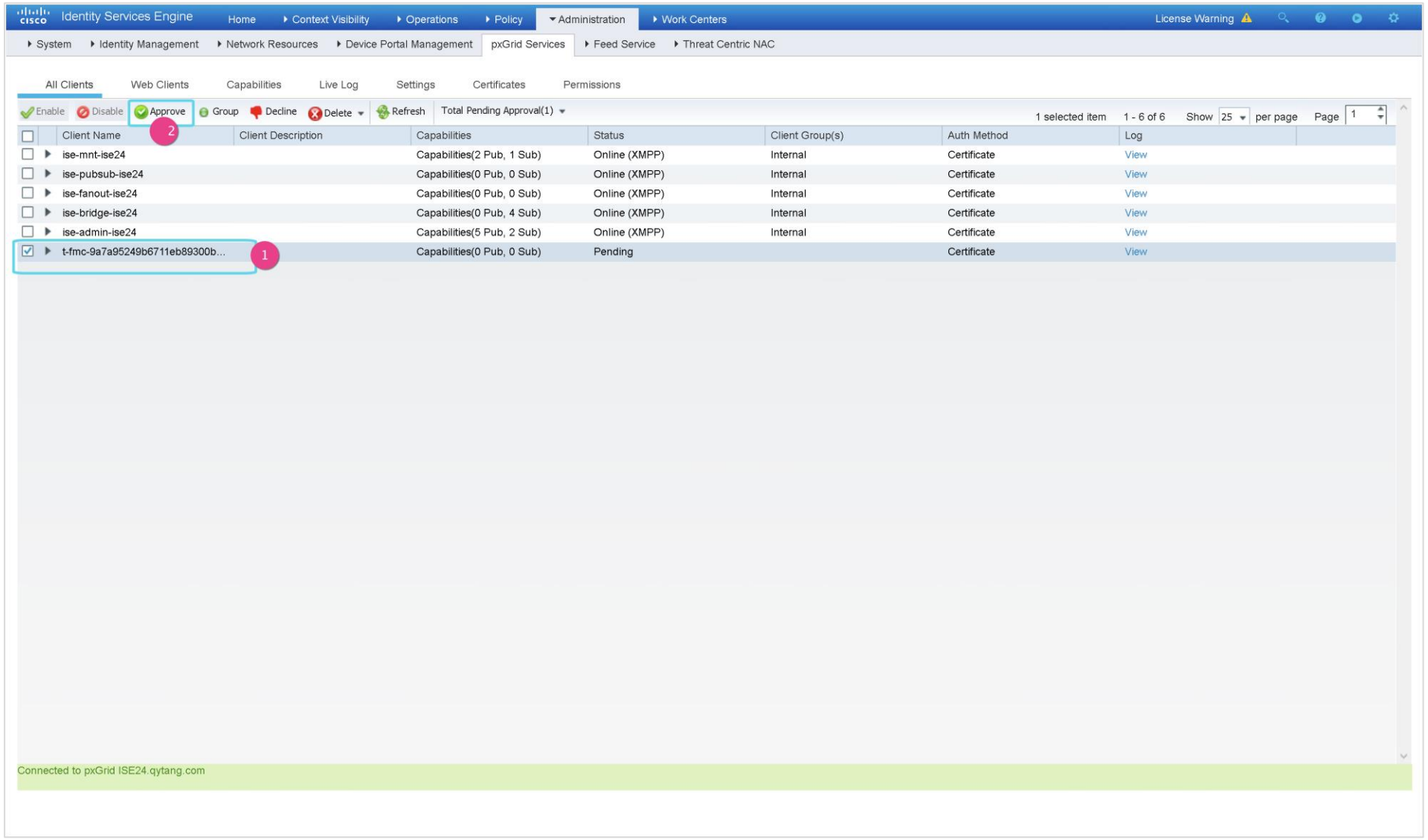
FMC与ISE之间的PxGrid(证书)



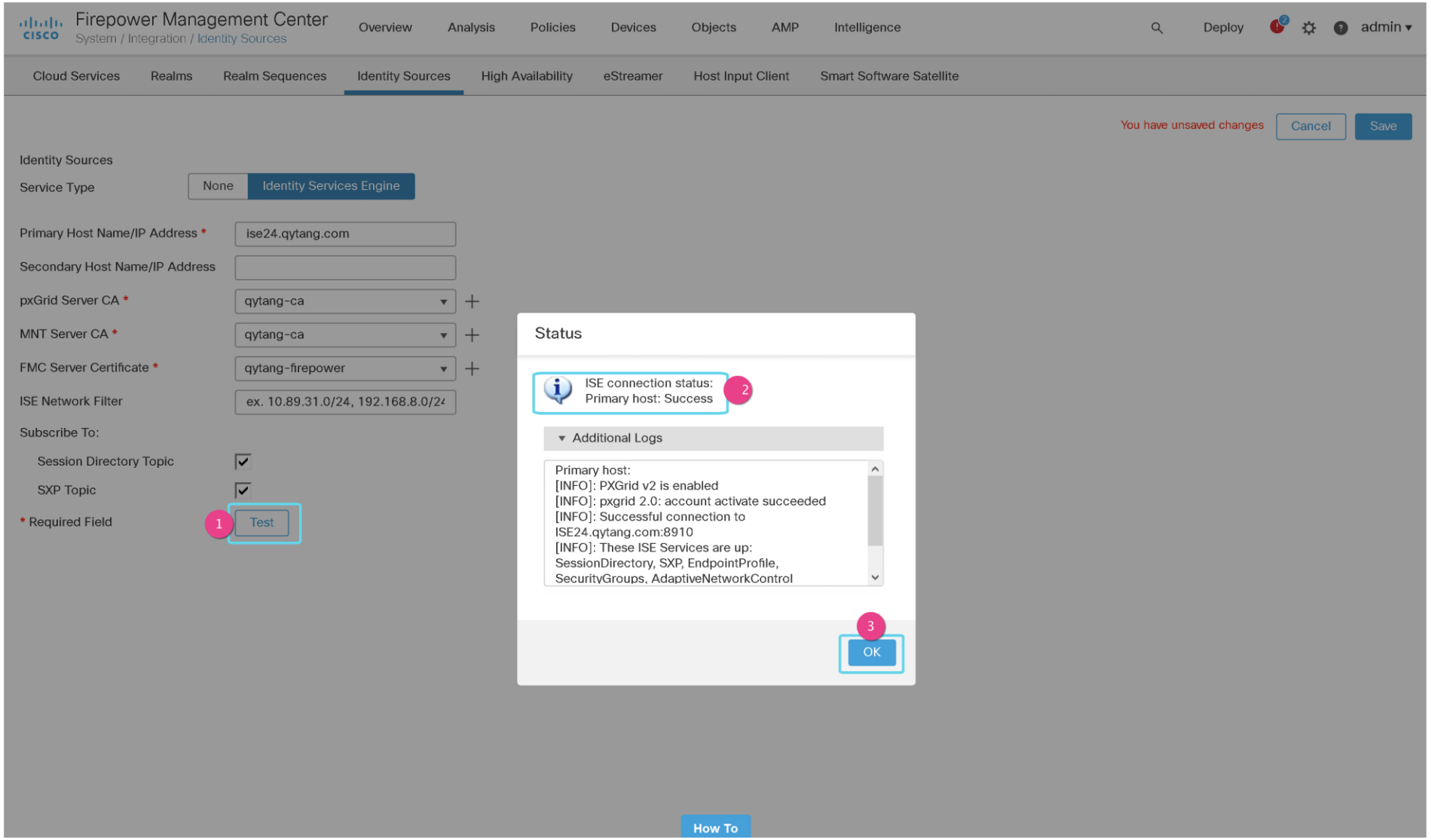
FMC与ISE之间的PxGrid(整合)



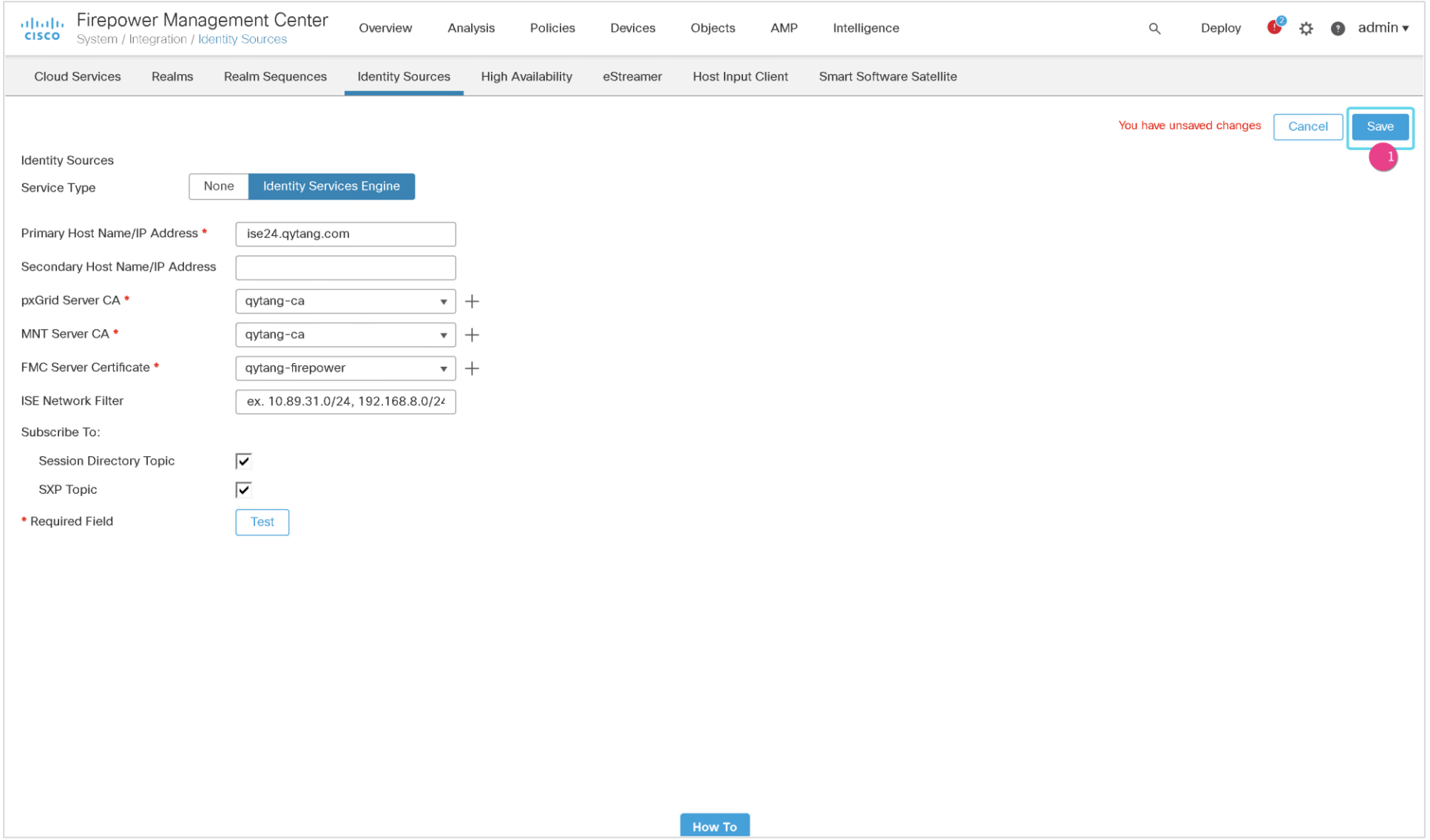
FMC与ISE之间的PxGrid(整合)



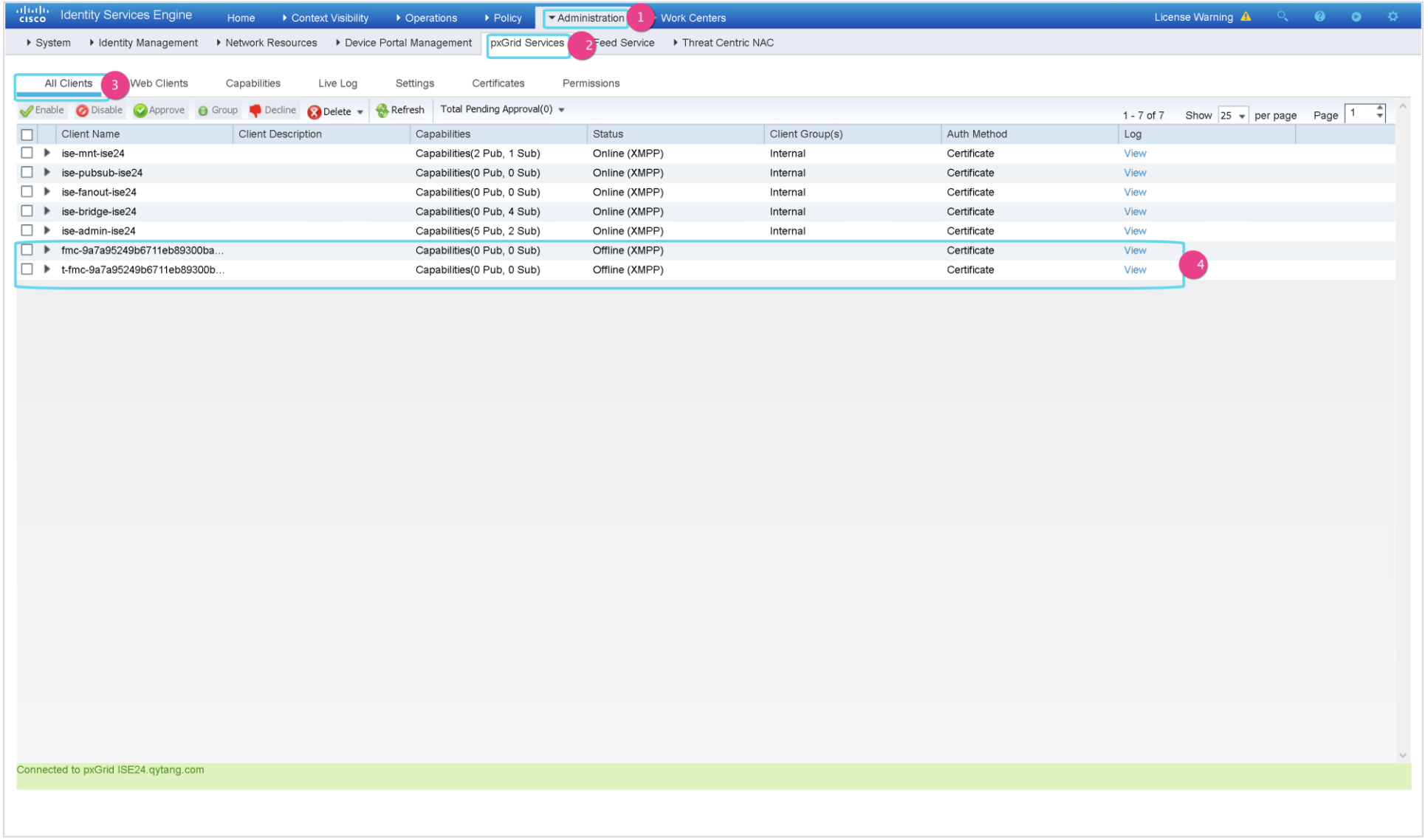
FMC与ISE之间的PxGrid(整合)



FMC与ISE之间的PxGrid(整合)



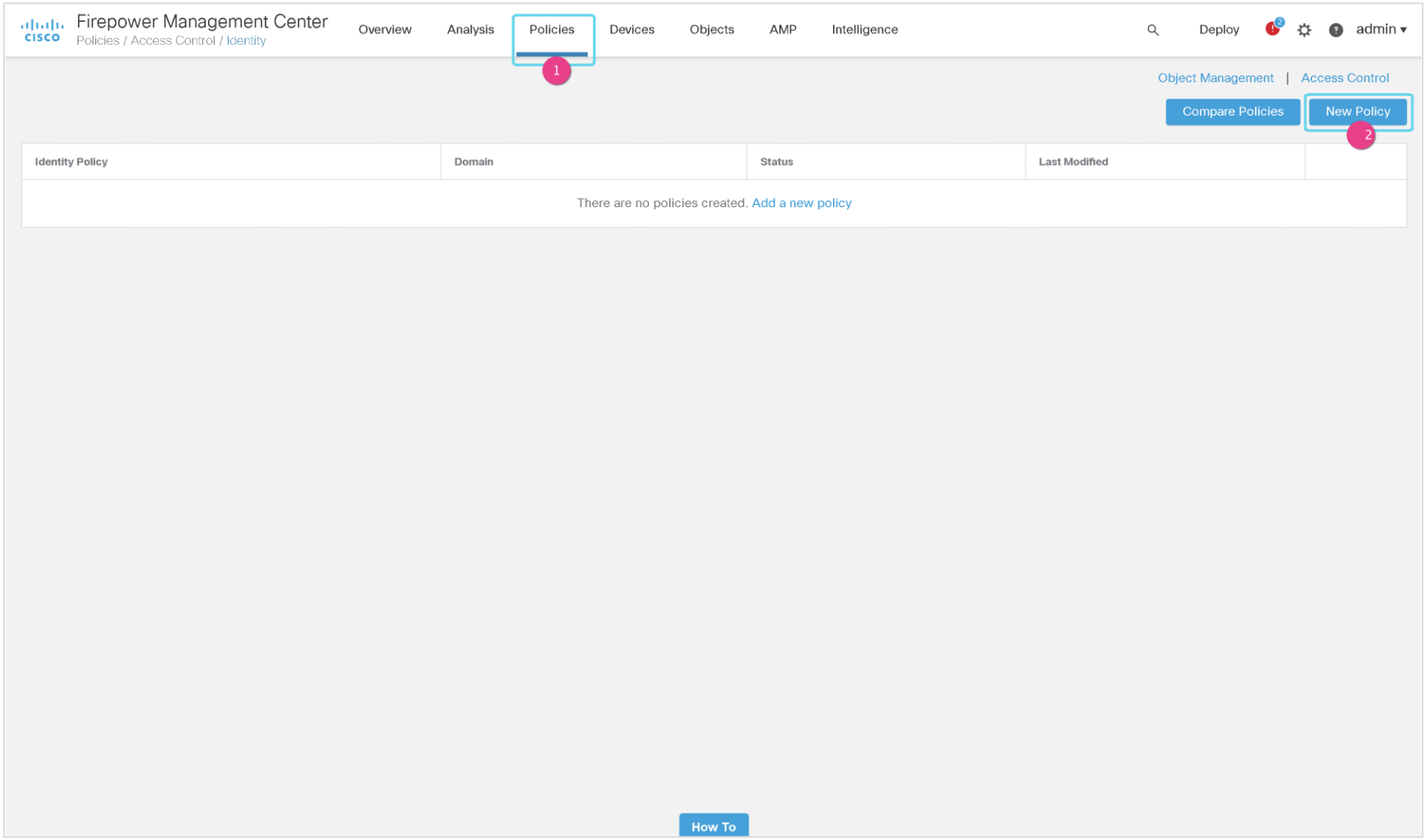
FMC与ISE之间的PxGrid(整合)



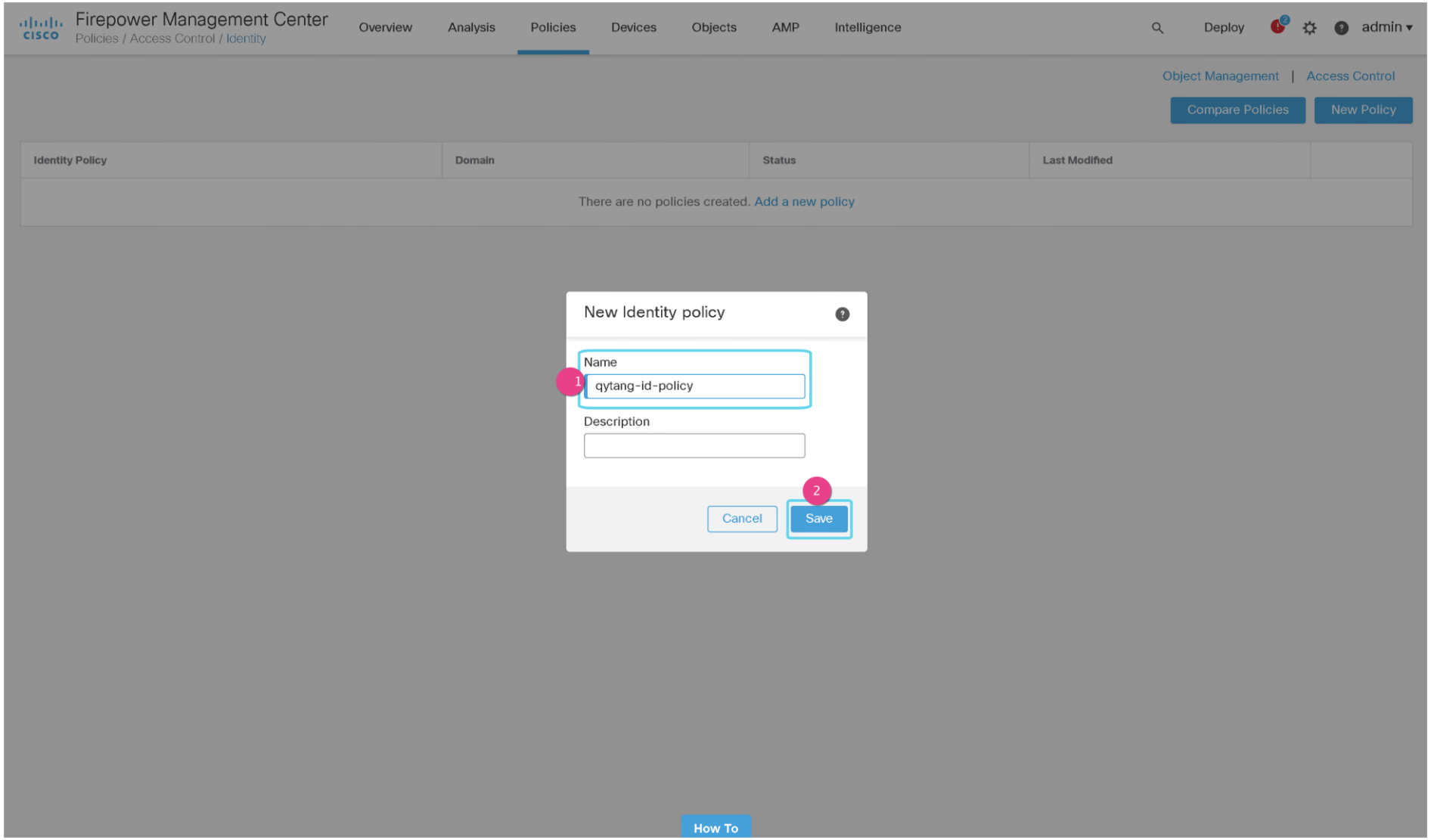
乾颐堂

4. FMC策略

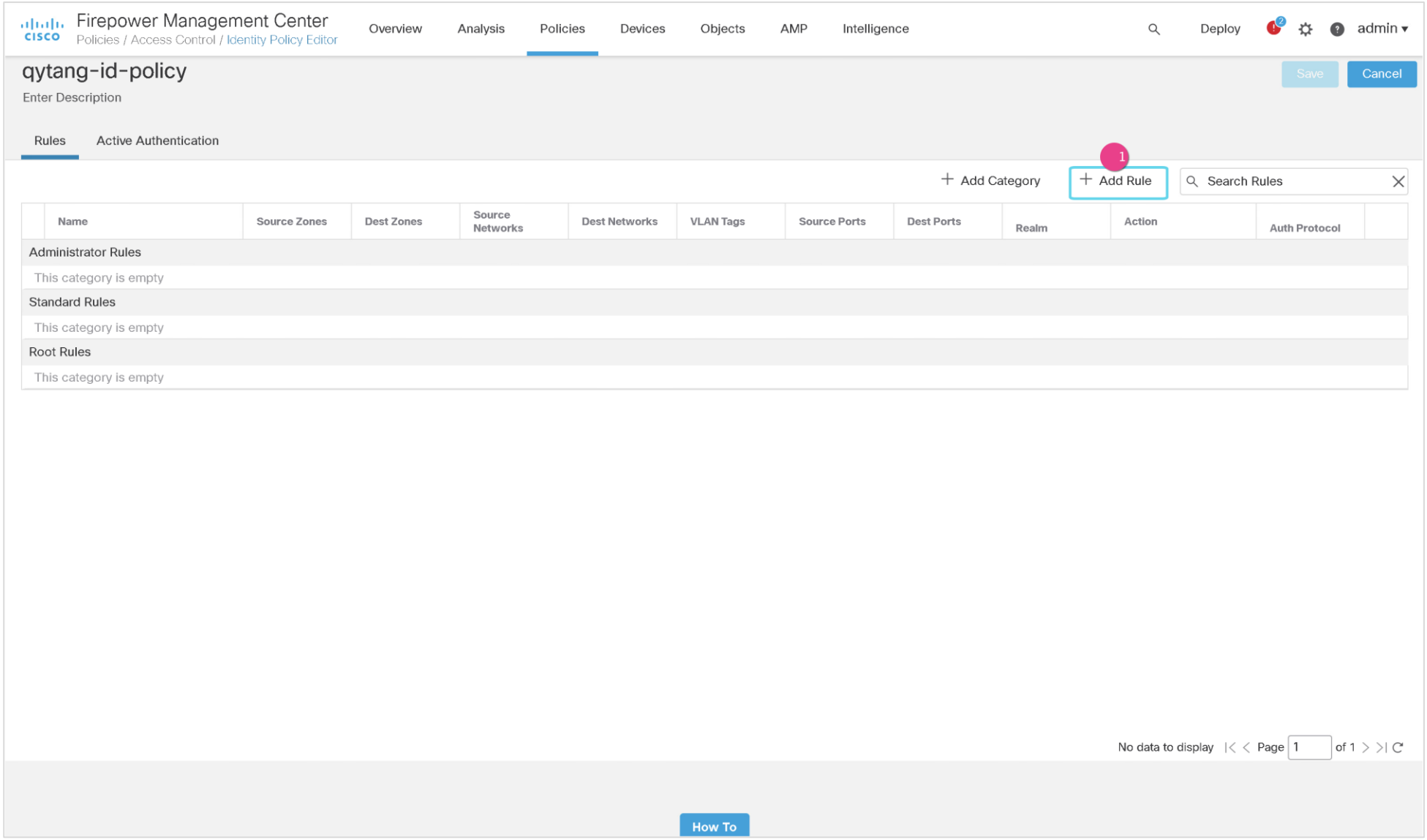
创建Identity策略



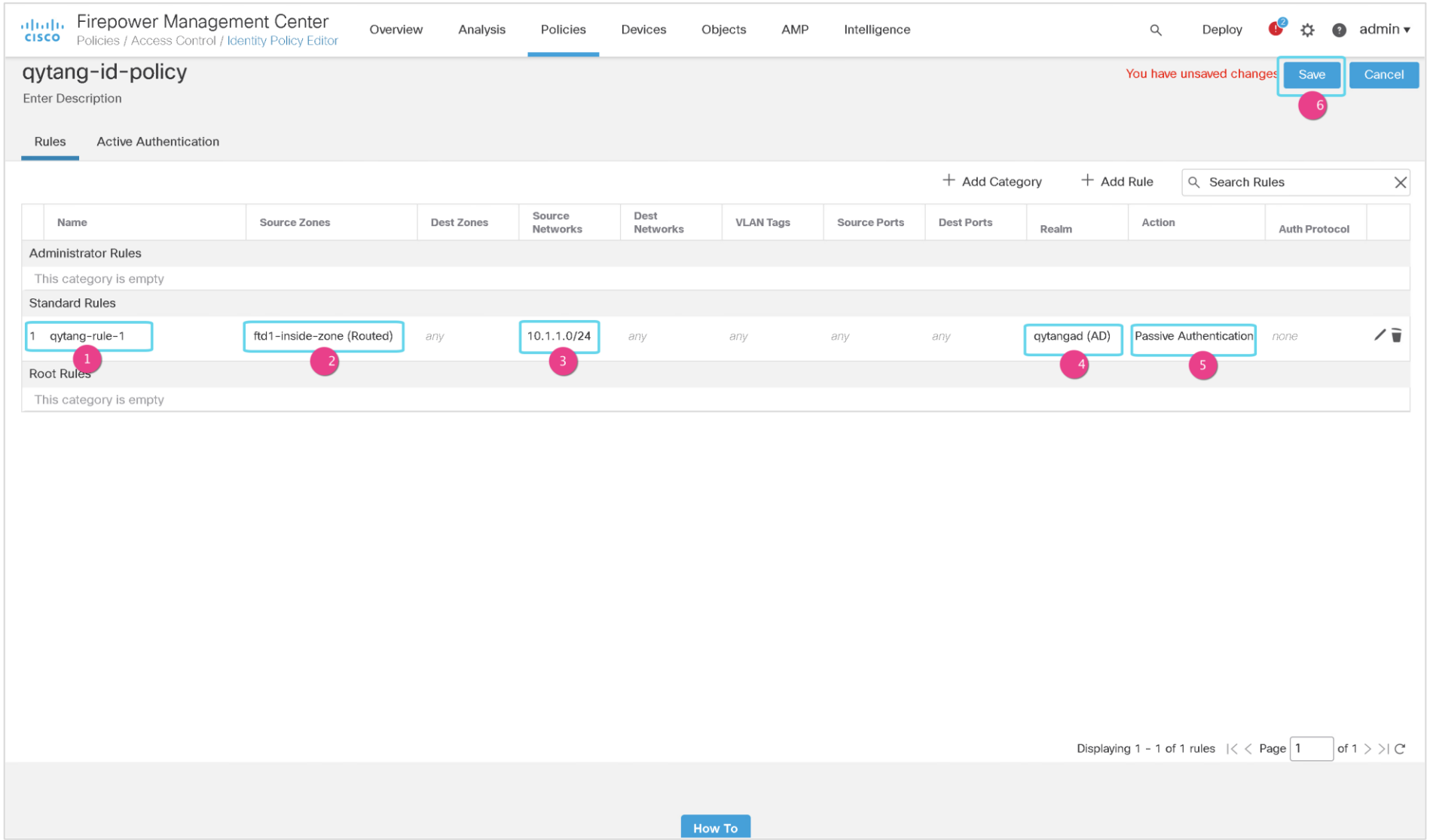
创建Identity策略



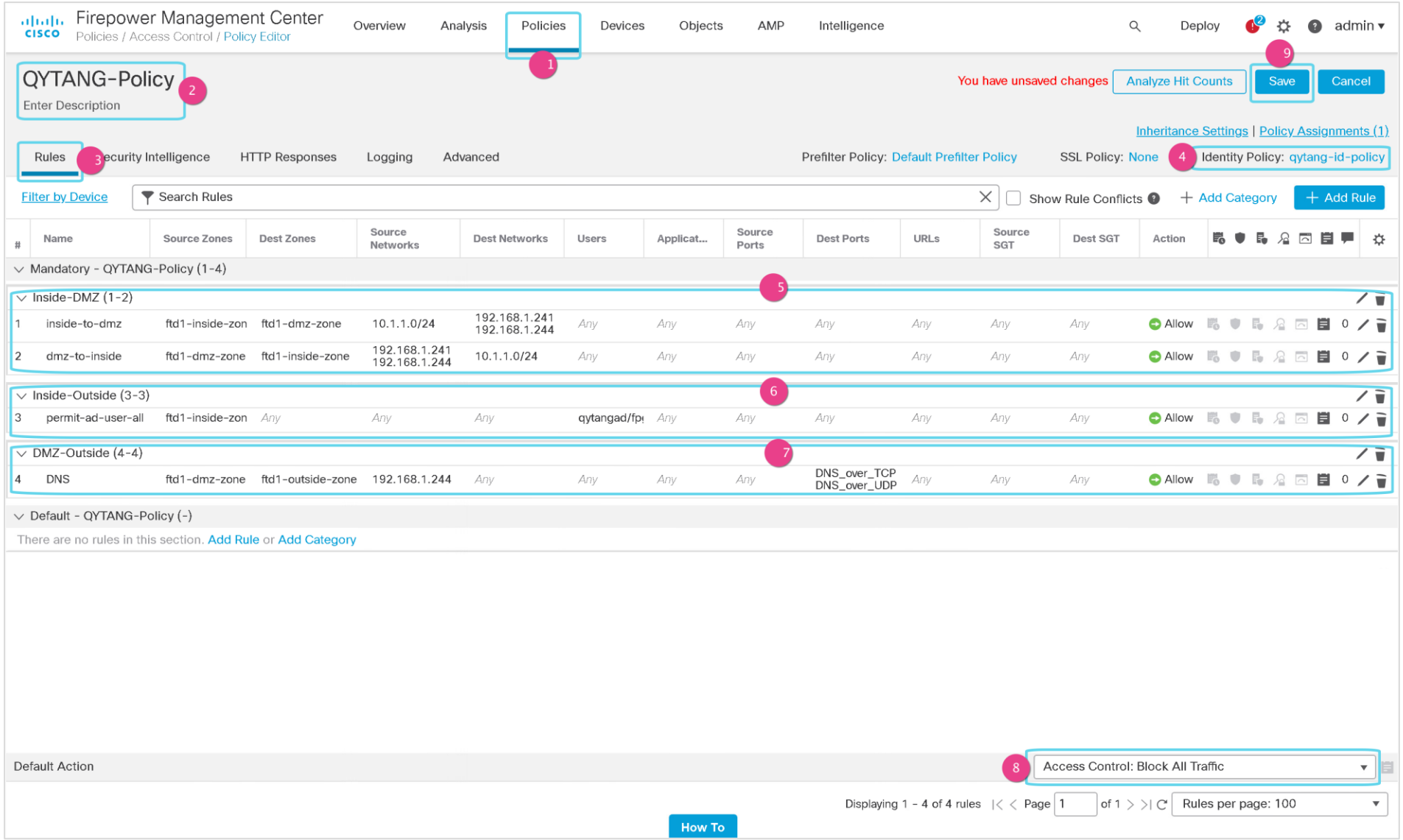
创建Identity策略



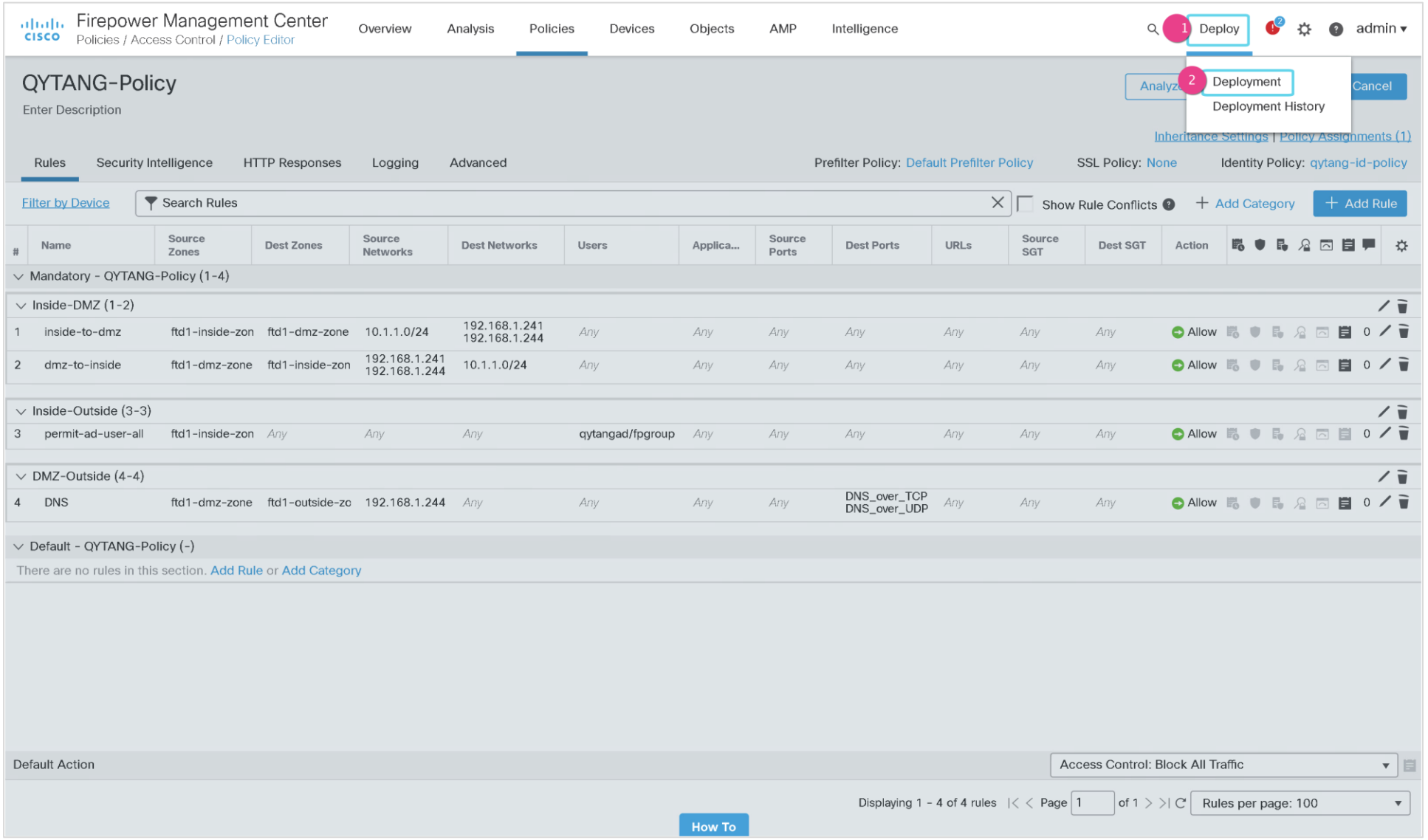
创建Identity策略



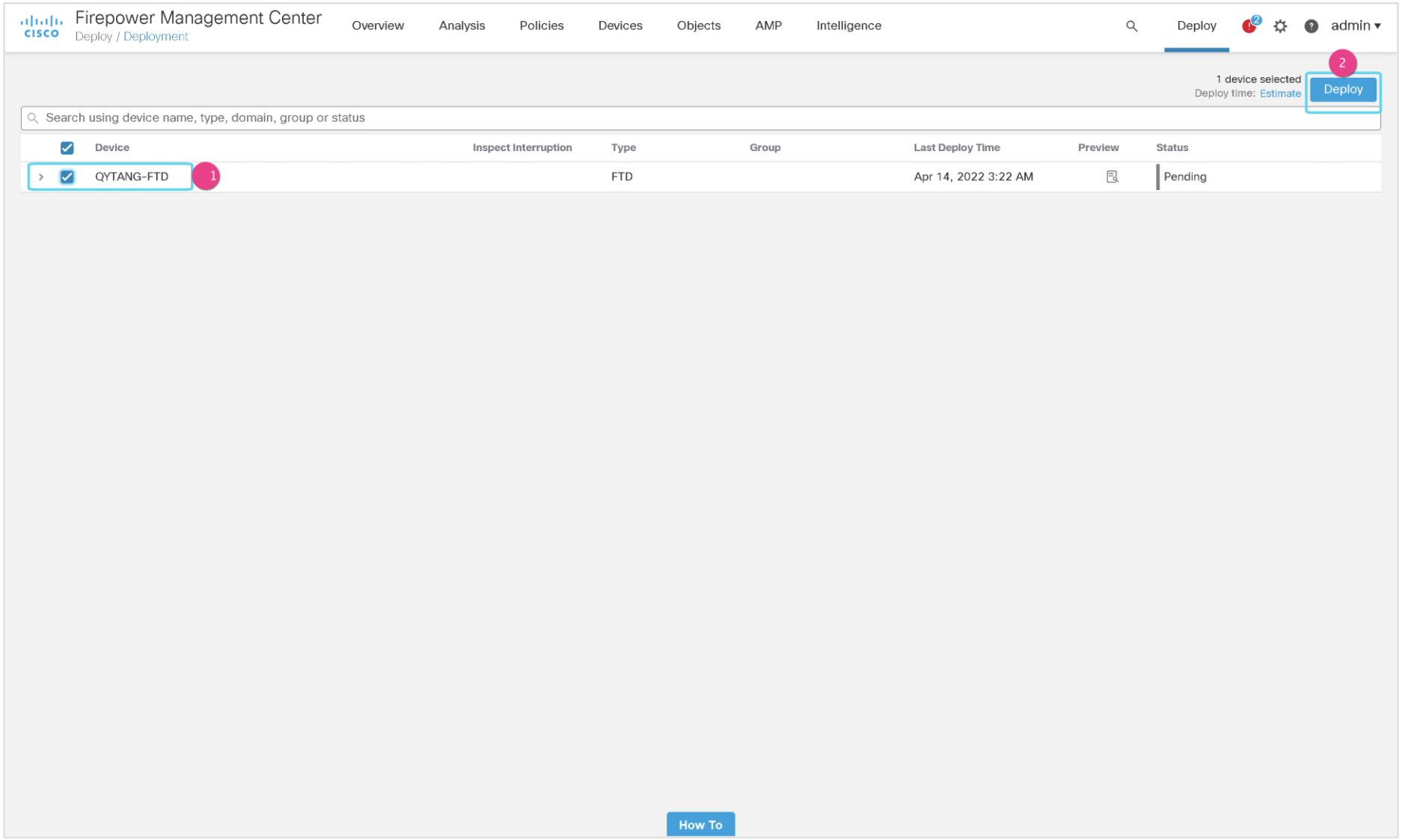
Access策略



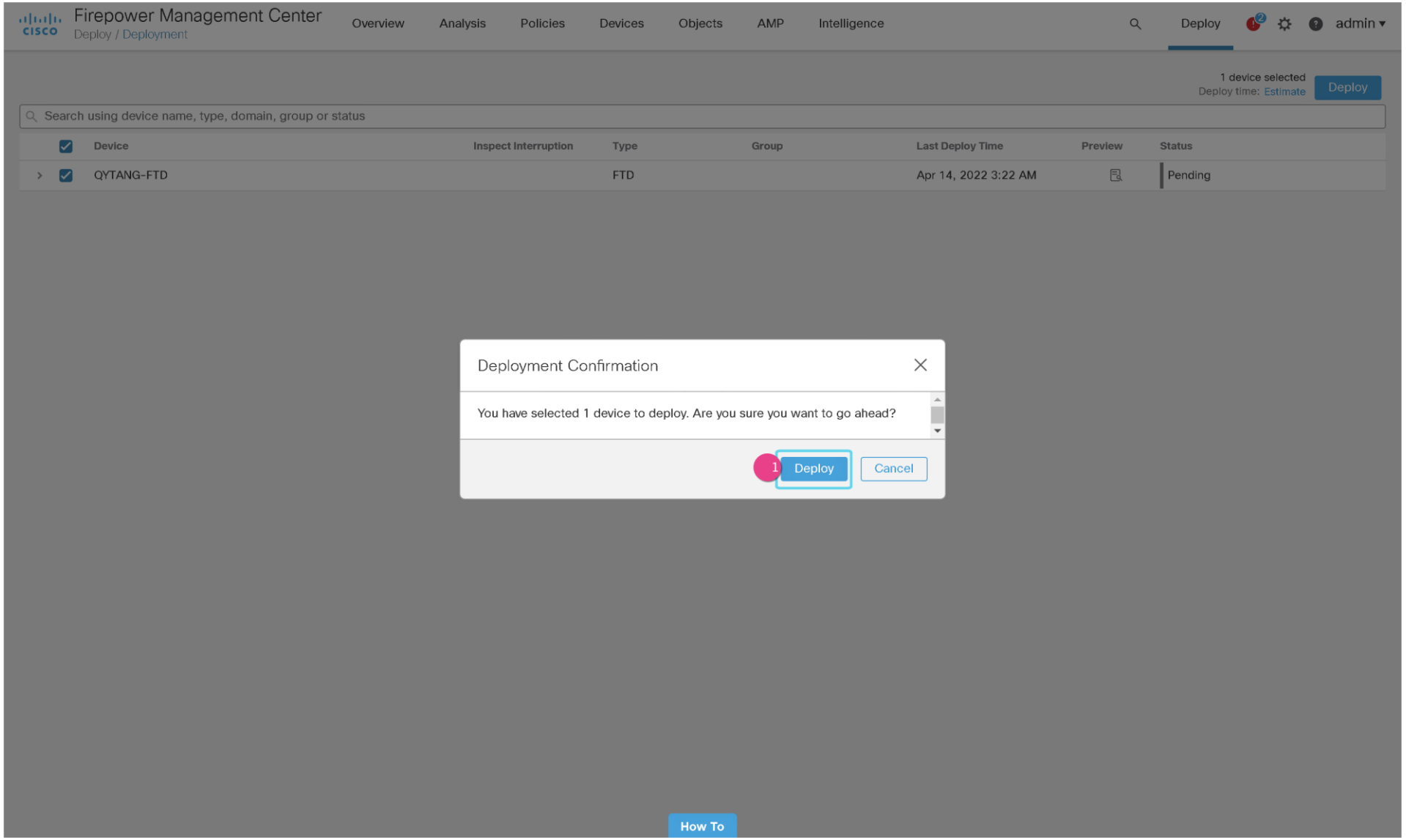
Access策略



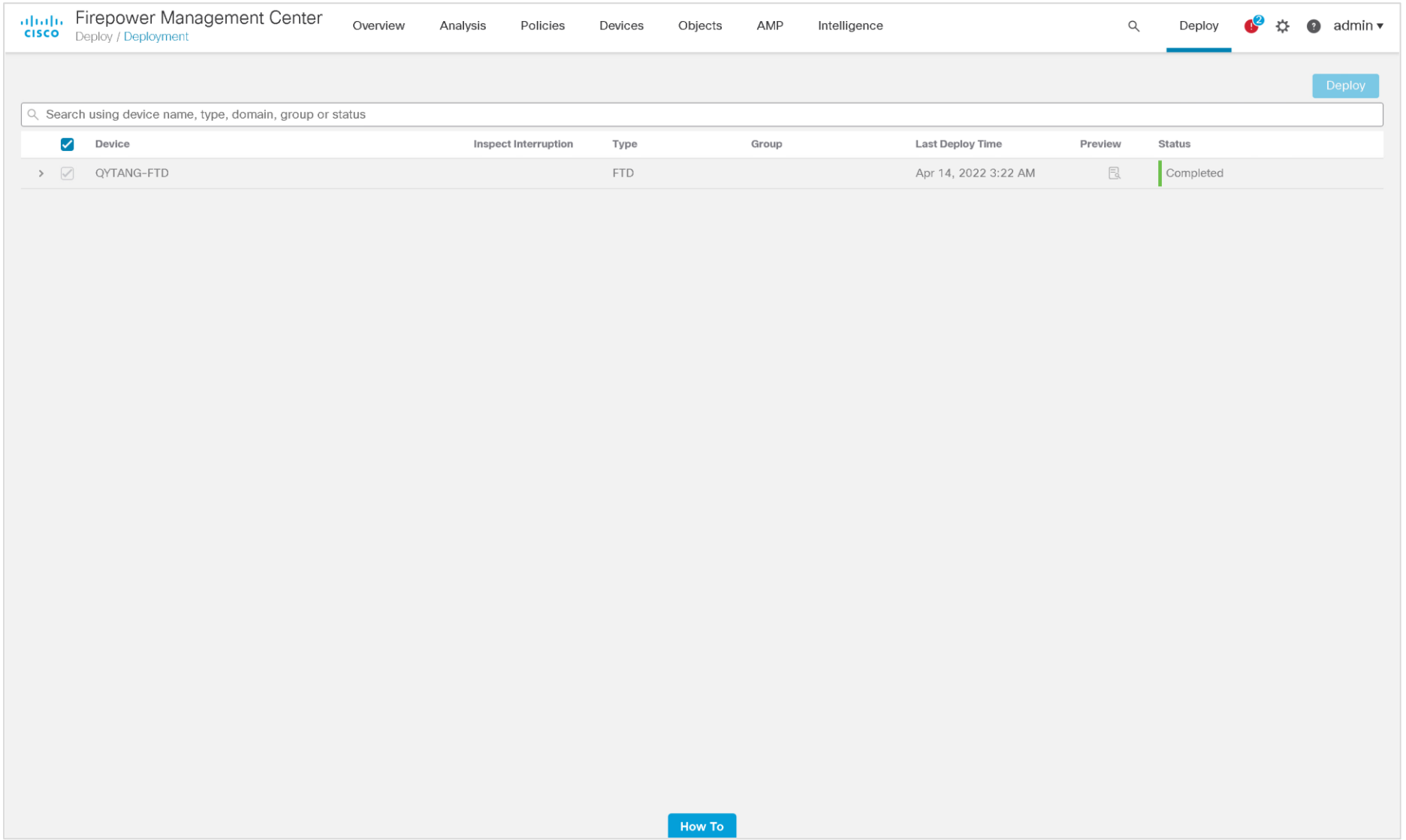
Access策略



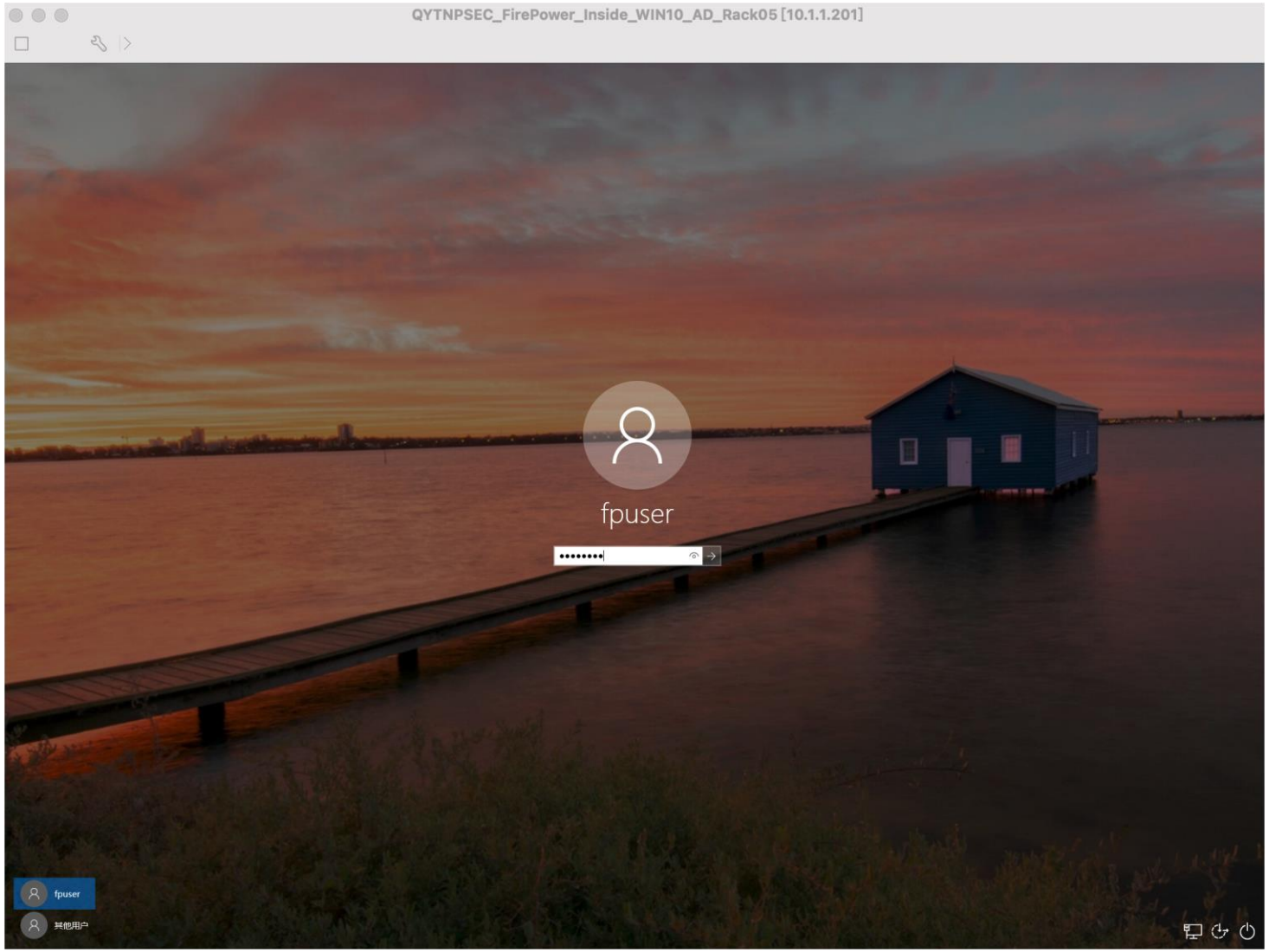
Access策略



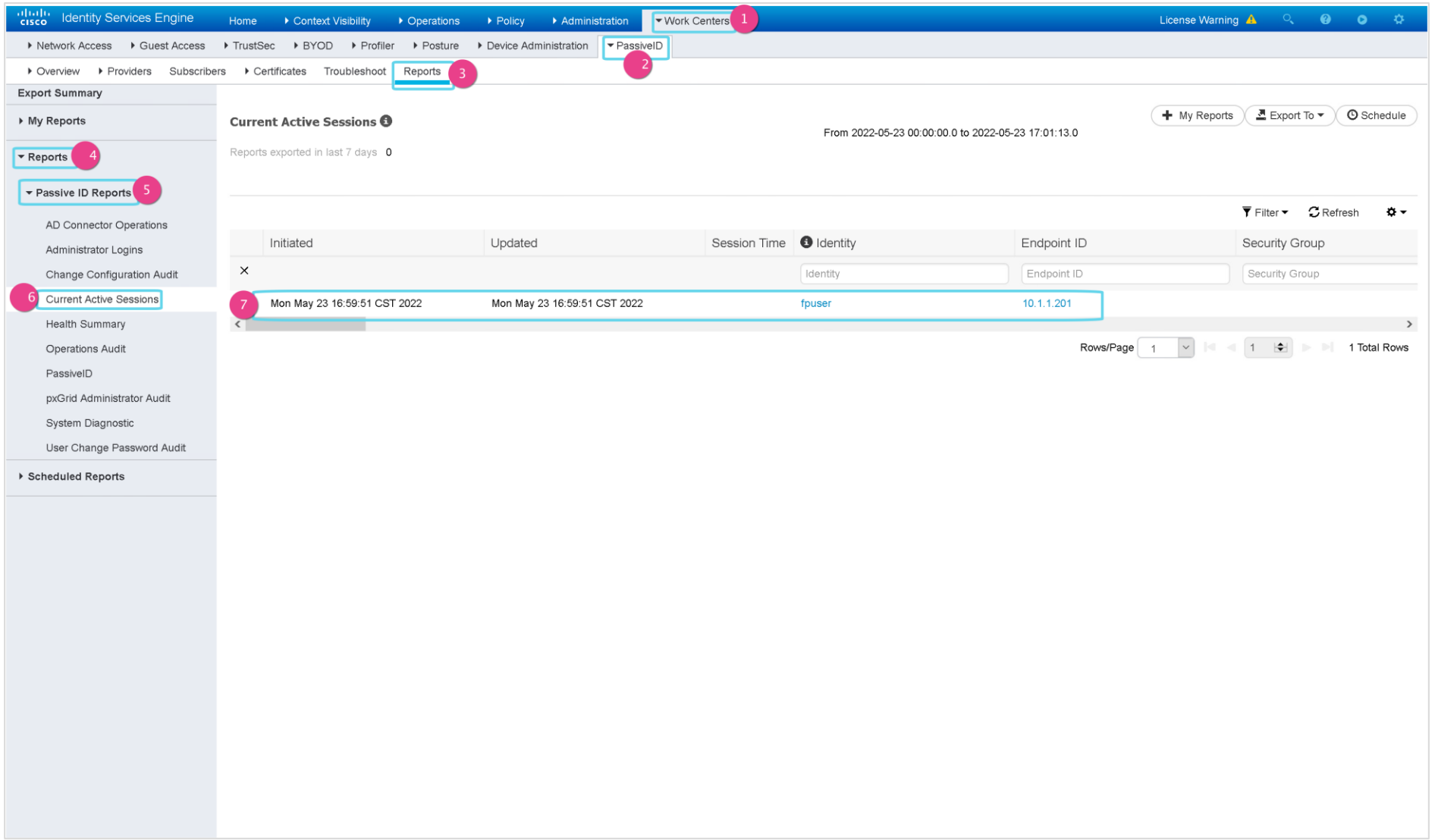
Access策略



测试(登录域)



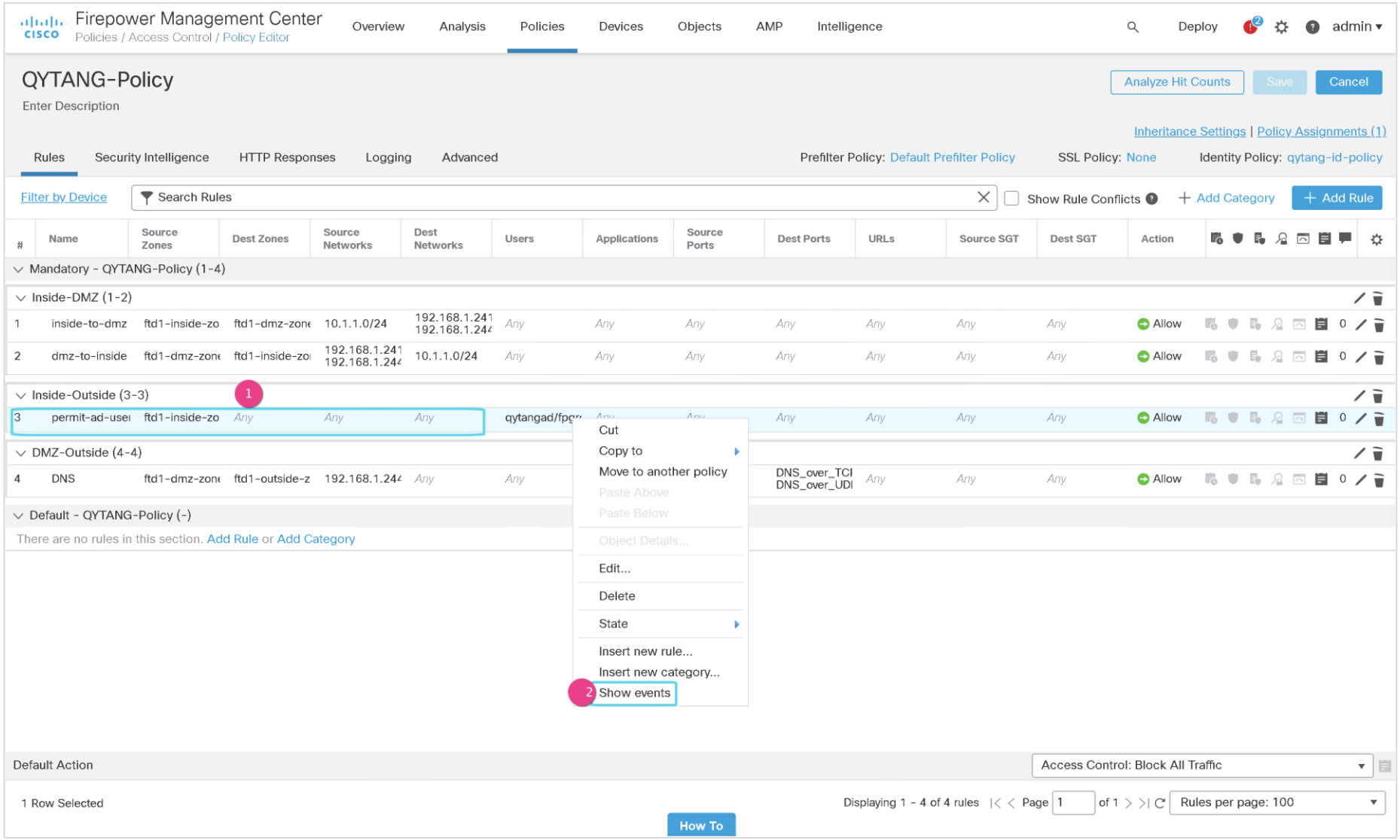
测试(查看Current Active Session)



测试(访问互联网)


baidu.com/s?ie=utf-8&f=8&rsv_bp=1&rsv_idx=1&tn=baidu&wd=qytang&fenlei=256&rsv_pq=bc918a8600054a0e&rsv_t=124c1ZuRHcINX7h%2BhlazM%2ByDWk8Bk%2BkA8hKd61jCc76YQNg7xu8tZkxwK1HJ&rqlang=en&rsv_enter=1&rsv_dl=tb&rsv_sug3=7&rsv_sug1=1&rsv_sug7=1...
qytang
百度一下
百度首页
设置
登录
网页 图片 文库 视频 资讯 贴吧 知道 采购 地图 更多
百度为您找到相关结果约295,000个
搜索工具
山石网科防火墙接入方式之透明模式 - 百度文库
2页 发布时间: 2018年07月01日
QYTANG(config)# int e0/1 QYTANG(config-if-eth0/1)# zone l2-trust QYTANG(config-if-eth0/1)# no shutdown QYTANG(config-if-eth0/1)# exit QYTANG(config)# int e0/2 QYT...
百度文库 保障 百度快照
乾颐堂Python网络快速强化班 - 乾颐堂网络实验室
第11周:5月13-19 Python网络编程 网络监控与自动化运维 第12周:5月20-26 Python网络编程 网络监控与自动化运维 乾颐堂客服热线:400-618-8070 乾颐堂官网:www.qytang.com 乾颐...
乾颐堂网络实验室 保障 百度快照
专注思科培训_Python培训_CCIE培训_HCIE培训 - 乾颐堂网络...
【乾颐堂网络实验室】专注思科培训,华为培训,Python培训【来电咨询:400-618-8070】涵盖CCNA培训、CCNP培训、CCIE培训、HCIE培训、HCIP培训、HCIA培训,CCIE安全培训、DC数据中心培训,及思科华为考...
乾颐堂网络实验室 保障 百度快照
河南泉源堂智慧药房连锁有限责任公司 - 爱企查
2022年5月12日 官网:www.qytang.cn 地址:郑州经济技术开发区航海东路与第二十五大街交叉口联东U谷第一期东区35号楼2层35-2-1 简介: 河南泉源堂智慧药房连锁有限责任公司成立于2021年03月18日,注册...
爱企查 百度快照
仓库- 现任明教教主-乾颐堂 (qytang) - Gitee.com
@qytang 乾颐堂创始人秦柯|网名现任明教教主! 关注私信 0 Stars 37 Watches 381 Followers 0 Following http://weibo.com/xrmjjz http://weibo.com/xrmjjz 概览仓库34星选集 ...
gitee 保障 百度快照
其他人还在搜
37tang 彩名堂 鸡汤 Tang Duy Tan Xtandi 黄糖 qy1005 qy是谁 trakatan KHITAN
乾颐堂现任明教教主网络入门到实战课程! - 乾颐堂网络实验室
思科,华为,Python学习 CCNA|CCNP|CCIE|HCIA|HCIP|HCIE 路由交换|安全|DC数据中心|无线|云计算 乾颐堂客服热线:400-618-8070 乾颐堂官网:www.qytang.com 乾颐堂网络实验室 我们为您想的更多
new.qytang.com/Timetable/view/... 百度快照
现任明教教主-乾颐堂 (qytang) - Gitee.com
qytang_Python 乾颐堂Python学习 Python 164040 Python_Network_2018_HTTP 2423 PyQYT 乾颐堂乾颐盾Python网络编程PyQYT项目 Python 3817 VIP_LDAP3 4513 DevNet2019 2215 El...
Gitee 保障 百度快照
qytang的空间 - 播种网
qytang的个人空间http://rili.bozhong.com/286106.html[收藏][复制][分享][RSS] 空间首页 动态 记录 日志 相册 主题 分享 好友 个人资料 头像 加为好友 给我留言 打个招呼 发...
播种网 百度快照
百度热搜
换一换
确保夏粮颗粒归仓
1 拜登启动印太经济框架 13国加入 热
2 朝鲜元帅国葬出殡 金正恩为其抬棺 热
3 "动态清零"可持续且必须坚持 热
4 北京24小时新增本土感染者63例 新
5 河南隔一天测一次核酸 费用谁出？
6 清华在校女博士报考协警未被录取
7 拜登保镖在韩国打人后紧急回国
8 日本首相：日美将监视中国海军活动 新
9 世卫发布猴痘疫情暴发预警 热
10 订单转移东南亚 外贸寒冬来了吗
11 王心凌回应又火了
12 张文宏：新冠疫情短期内不会结束 热
13 瞒报行程致疫情在京扩散 工头致歉 热
14 3米长抹香鲸2次搁浅沙滩死亡
15 居民错过核检被要求补缴前24轮费用

测试(查看日志)



测试(查看日志)