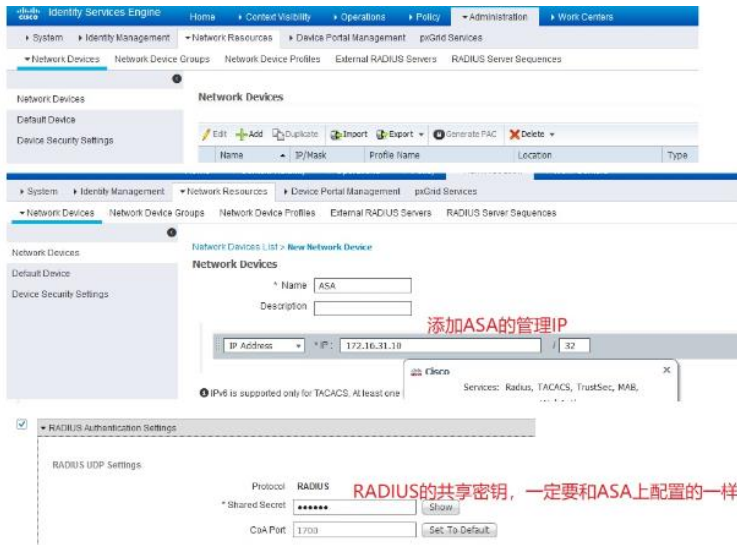


## ISE 配置部分

### 1. 添加 ASA 到 ISE 为 RADIUS 客户端

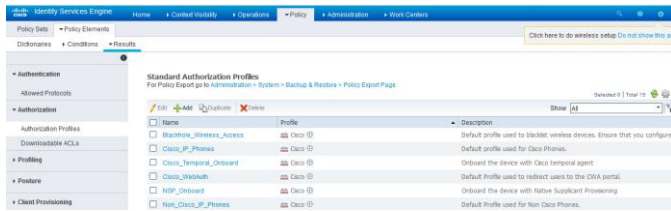
Administration---Network Resource---Network device ,然后 add,填写 ASA 的 MGT IP 和 RADIUS 的 share key



The screenshot shows the ISE Administration console for configuring a new network device. The 'Network Devices List' section is active, and a 'New Network Device' form is displayed. The 'Name' field is set to 'ASA'. The 'IP Address' field is set to '172.16.31.10'. The 'RADIUS Authentication Settings' section is expanded, showing the 'Protocol' set to 'RADIUS' and the 'Shared Secret' field filled with asterisks. Red annotations in Chinese are present: '添加ASA的管理IP' (Add ASA management IP) points to the IP address field, and 'RADIUS的共享密钥,一定要和ASA上配置的一样' (RADIUS shared key, must be the same as configured on ASA) points to the shared secret field.

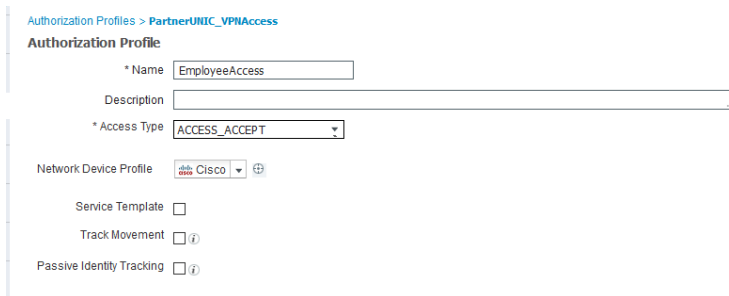
### 2. 添加 Authorization profile

Policy--Policy Elements --Result ---Authorization----Authorization profile---add



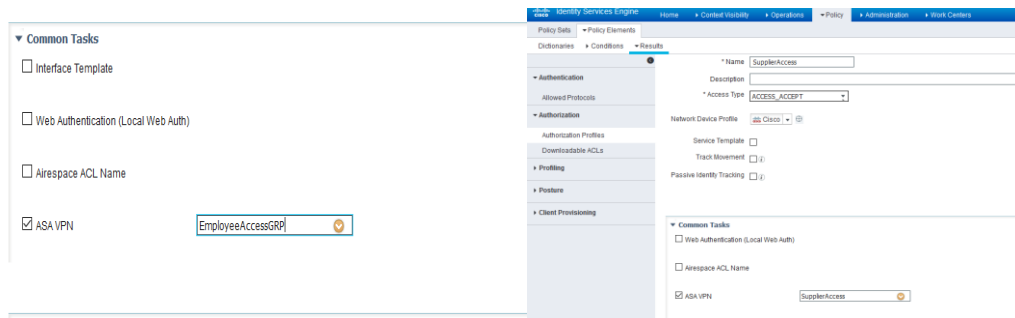
The screenshot shows the ISE Administration console for the 'Policy Elements' section. The 'Authorization' tab is selected, and a table of 'Standard Authorization Profiles' is displayed. The table has columns for 'Name', 'Profile', and 'Description'. Several profiles are listed, including 'Baseline\_Wireless\_Access', 'Cisco\_IP\_Phones', 'Cisco\_Temporal\_Override', 'Cisco\_WireAuth', 'NIP\_Override', and 'Non\_Cisco\_IP\_Phones'. The 'Name' field in the table is highlighted.

分别添加名为 EmployeeAccess 和 SupplierAccess 的 Authorization profile



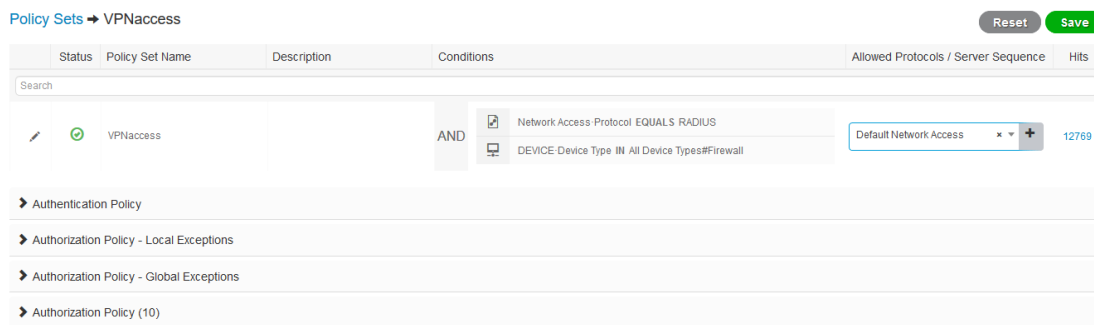
The screenshot shows the ISE Administration console for configuring an 'Authorization Profile'. The 'Name' field is set to 'EmployeeAccess'. The 'Access Type' dropdown is set to 'ACCESS\_ACCEPT'. The 'Network Device Profile' dropdown is set to 'Cisco'. Other fields like 'Description', 'Service Template', 'Track Movement', and 'Passive Identity Tracking' are visible but not filled.

在 Common task 的 ASA VPN 后面填入在 ASA 上定义的 group policy : EmployeeAccessGRP 和 SupplierAccessGRP (这个名字一定要和 ASA 上的一样)



#### 4. 添加认证的授权策略 Policy Sets

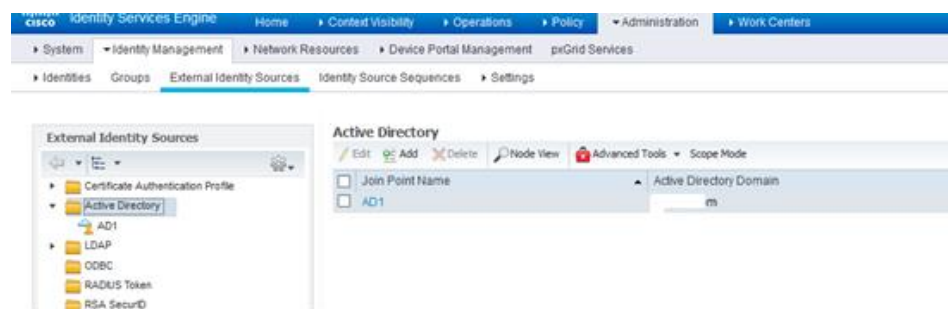
Policy--Policy Elements--Add ，添加名字为 VPNAccess 的认证策略  
 此例中，我选的条件为:protocol=radius ,和 device type=Firewall



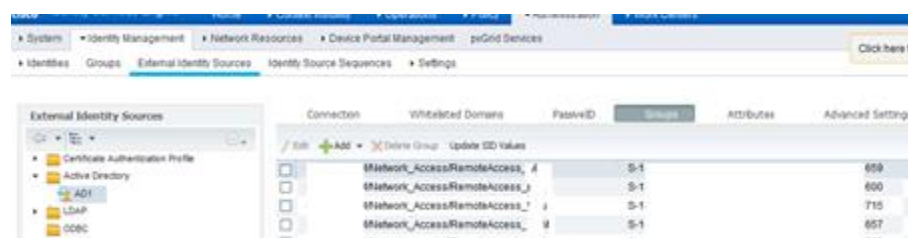
#### 5. 添加授权策略

在添加此策略之前，需要先将 ISE 加入企业内部的域

Administration—External Identity Sources—Active Directory--add



加入域后，点 AD1，然后在 AD group 从 AD 的安全组中添加企业员工和供应商 VPN 帐号所在的安全组



然后添加授权策略：

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Policy Elements [Click here to do wireless setup. Do not show this again.](#)

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions	
		1_VPNAccess_Authorized_	AND	AD1-ExternalGroups EQUALS C COMNetwork_Access RemoteAccess_	%EmployeeAccessGRP	Select from list	3530	
		2_VPNAccess_Authorized_	AND	DEVICE Device Type IN All Device Types#Firewall AD1-ExternalGroups EQUALS C COMNetwork_Access RemoteAccess_	%SupplierAccessGRP	Select from list	15	

此处分别选择AD上定义的企业员工和供应商的VPN组

此处分别选择前面定义的和ASA group policy 关联的授权配置文件