

ISE BYOD

Bring Your Own Device

| 主讲人：现任明教教主

| PPT制作：刘强龙



内容简介

1. BYOD简介
2. 基础网络,MS域与证书环境
3. ISE基本证书与域操作
4. WLC与ISE授权
5. BYOD测试



1. BYOD简介

Why ISE for BYOD?



Simple BYOD (Base License)



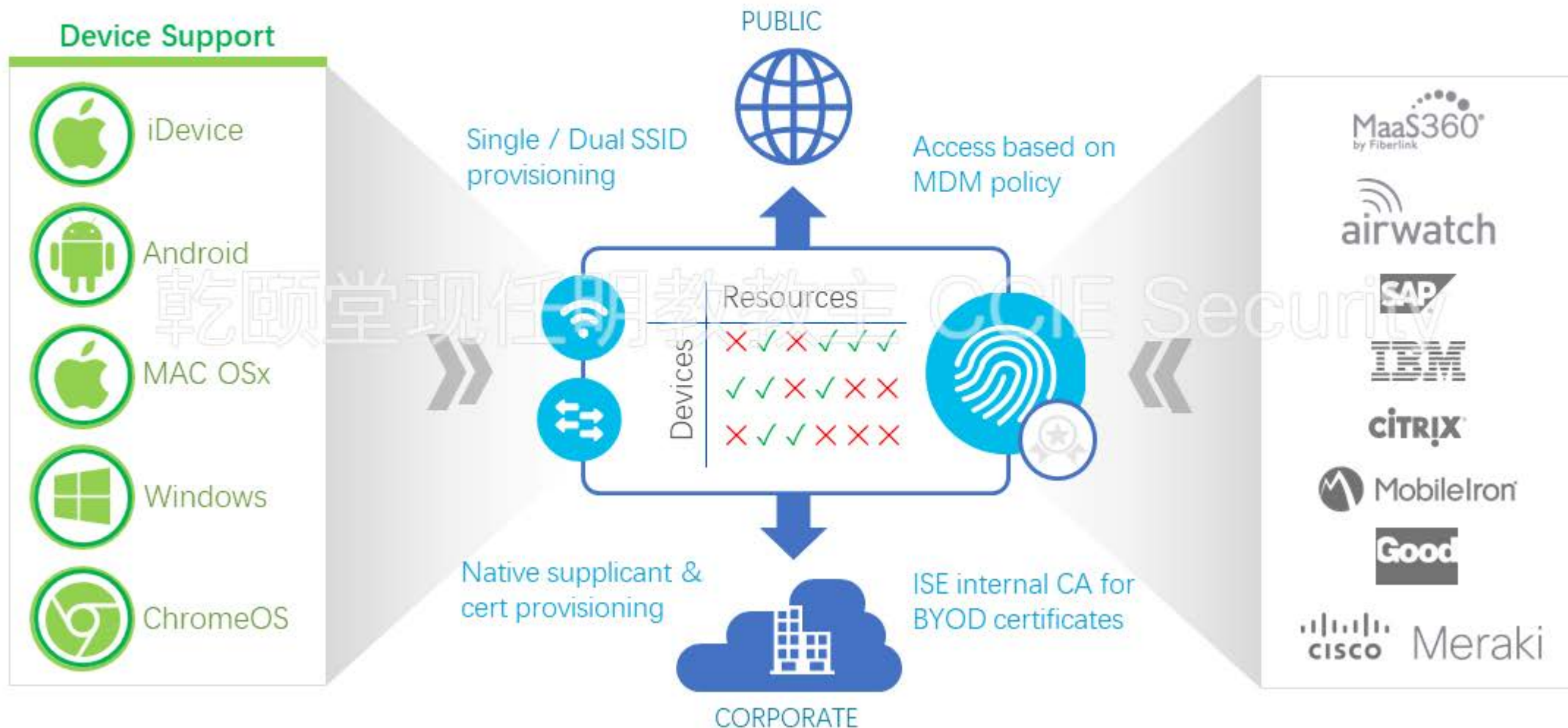
- **Guest type** 'internet only' access to personal device **Or**
- Password based access to BYOD SSID, limited access

Full BYOD (Base + Plus License)



- **Full automation** of BYOD process – Device registration, Native supplicant configuration, Certificate installation, manage.

ISE BYOD solution overview



Mobile device posture assessment

MDM Policy Checks

Device registration status

Device compliance status

Disk encryption status

Pin lock status

Jailbreak status

Manufacturer

Model

IMEI

Serial number

OS version

Phone number

Posture Compliance assessment for Mobile devices



AbsoluteSoftware

GLOBO

SAP

JAMF software

IBM

CISCO Meraki

Symantec

airwatch

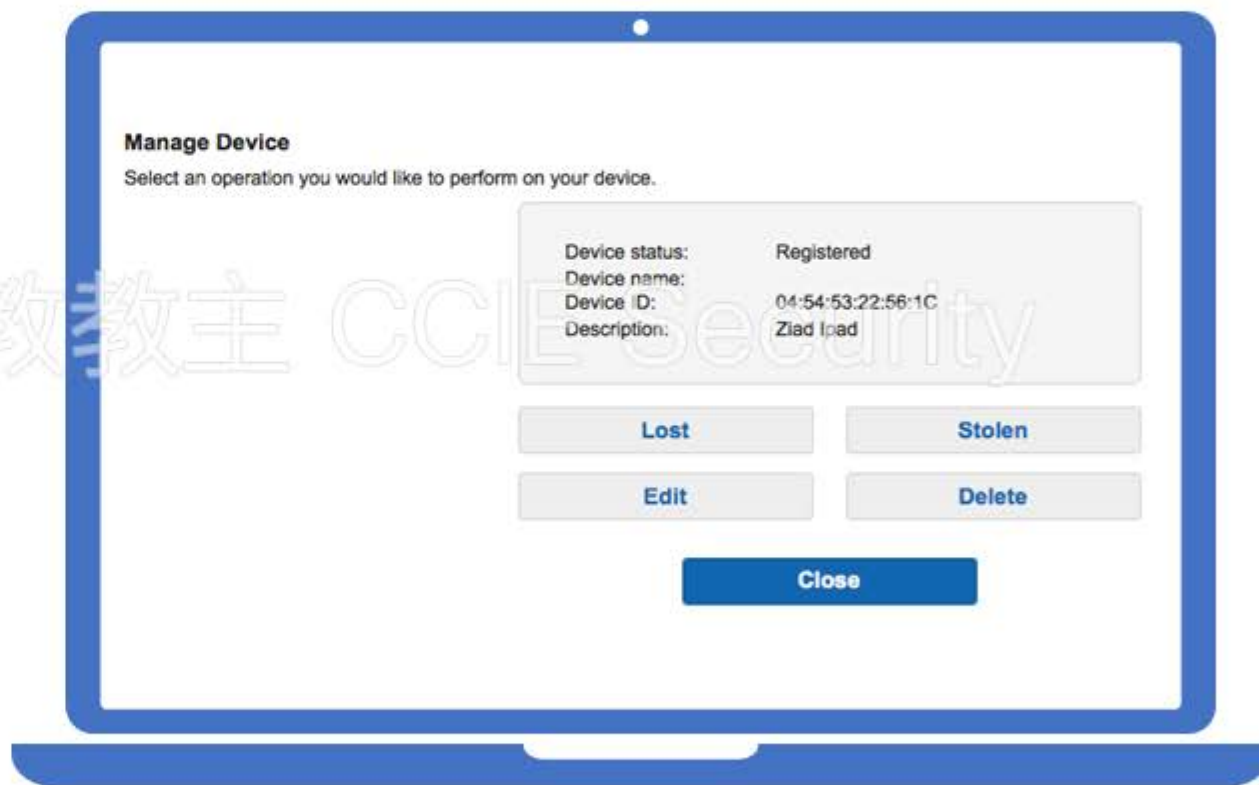
Tangoe

MaaS360 by Fibertink

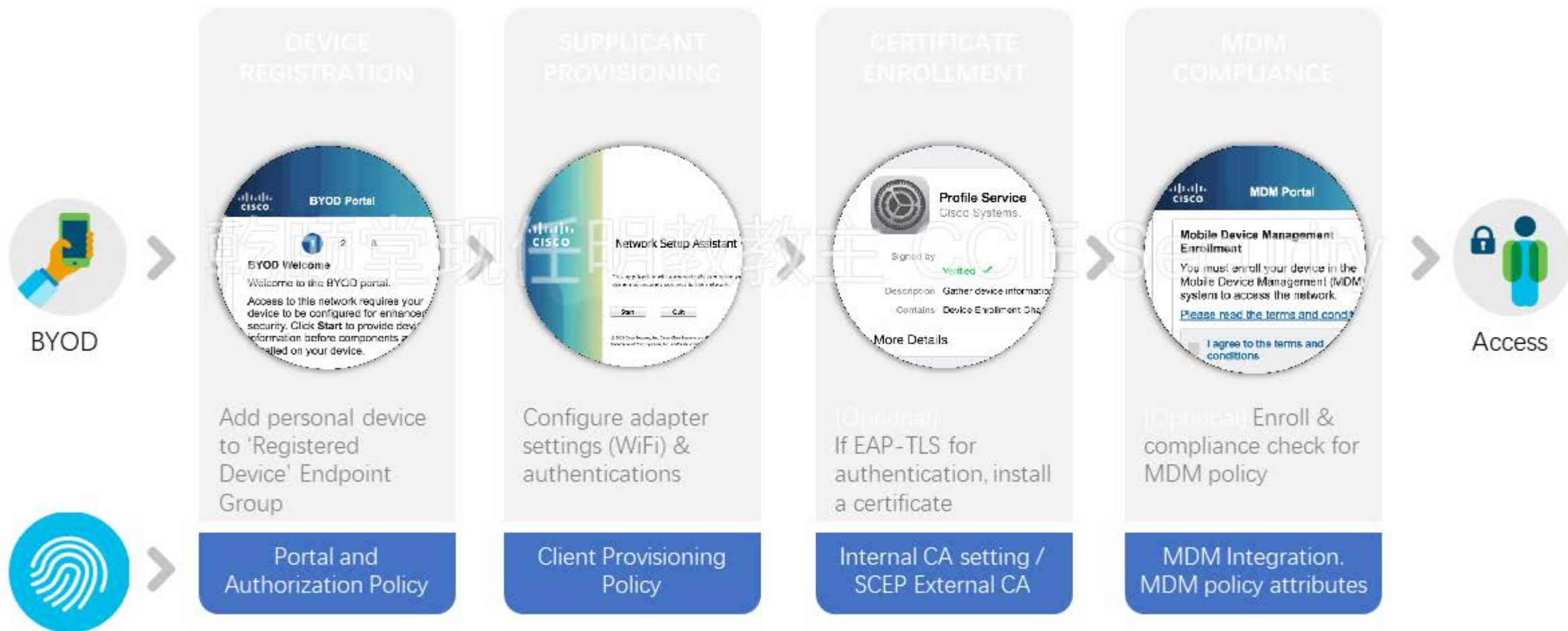
MobileIron

'My Devices' portal

- Users can **add their personal devices** in to the network (as fallback option to native supplicant provisioning)
- Users can **report lost / stolen personal assets**.
- **Lost / Stolen assets are blacklisted** and their access to network is automatically revoked.



ISE automates BYOD workflow





2. 基础网络,域与证书环境

2.1 基础网络

2.2 安装MS域

2.3 安装MS证书服务器

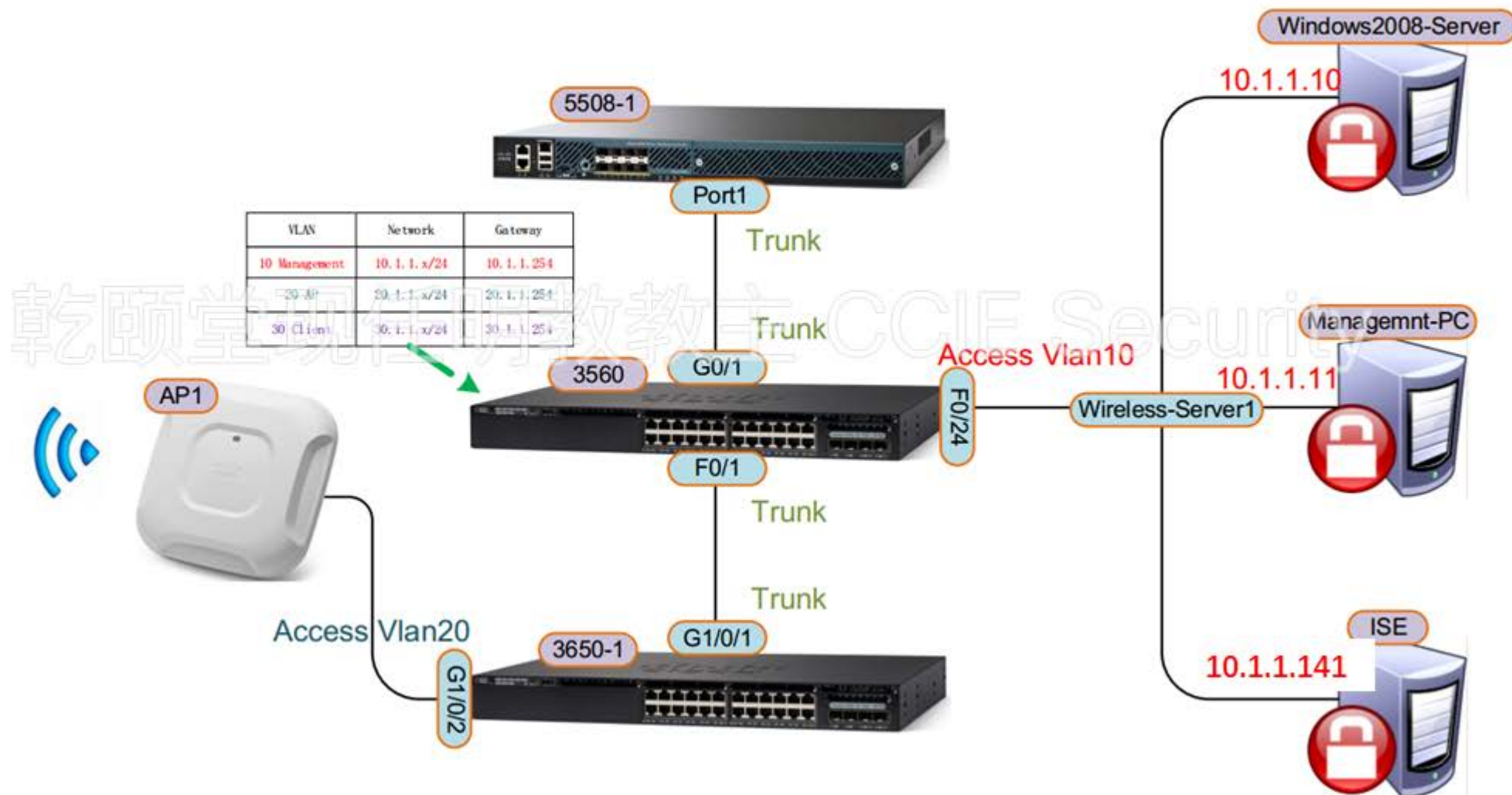
2.4 安装设备注册服务

2.5 创建注册单位,组和用户



2.1 基础网络

实验拓扑



SW3560 初始化

```
hostname SW3560
```

```
!
```

```
ip routing
```

```
!
```

```
ip dhcp pool client
```

```
network 30.1.1.0 255.255.255.0
```

```
default-router 30.1.1.254
```

```
dns-server 10.1.1.10
```

```
!
```

```
ip dhcp pool ap
```

```
network 20.1.1.0 255.255.255.0
```

```
default-router 20.1.1.254
```

```
option 43 hex f104.0a01.0164
```

```
!
```

```
interface FastEthernet0/24
```

```
switchport access vlan 10
```

```
switchport mode access
```

```
spanning-tree portfast
```

```
interface GigabitEthernet0/1
```

```
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
```

```
!
```

```
interface Vlan10
```

```
ip address 10.1.1.254 255.255.255.0
```

```
!
```

```
interface Vlan20
```

```
ip address 20.1.1.254 255.255.255.0
```

```
!
```

```
interface Vlan30
```

```
ip address 30.1.1.254 255.255.255.0
```

```
!
```

```
ip route 0.0.0.0 0.0.0.0 10.1.1.200
```

乾颐堂现任明教教主 ©CIE Security



3650-1 初始化

```
hostname 3650-1
```

```
!
```

```
vlan 20
```

```
name ap
```

```
!
```

```
interface GigabitEthernet1/0/2
```

```
switchport access vlan 20
```

```
switchport mode access
```

```
spanning-tree portfast
```

```
!
```

```
interface GigabitEthernet1/0/1
```

```
switchport mode trunk
```

乾乾堂现任明教教主 CCIE Security



初始化5508-1 (1)

System Name [Cisco_65:a6:a4] (31 characters max): WLC5508-1

Enter Administrative User Name (24 characters max): admin

Enter Administrative Password (3 to 24 characters): Cisc0123

Re-enter Administrative Password : Cisc0123

Service Interface IP Address Configuration [static][DHCP]:

Enable Link Aggregation (LAG) [yes][NO]:

Management Interface IP Address: 10.1.1.100

Management Interface Netmask: 255.255.255.0

Management Interface Default Router: 10.1.1.254

Cleaning up Provisioning SSID

Management Interface VLAN Identifier (0 = untagged): 10

Management Interface Port Num [1 to 8]: 1

Management Interface DHCP Server IP Address: 10.1.1.254

乾人 现任 明教 教主 CCIE Security



初始化5508-1 (2)

Enable HA [yes][NO]:

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: qytang

Network Name (SSID): qytang

Configure DHCP Bridging Mode [yes][NO]:

Allow Static IP Addresses [YES][no]:

Configure a RADIUS Server now? [YES][no]: no

Warning! The default WLAN security policy requires a RADIUS server.

Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]: CN



初始化5508-1 (3)

Enable 802.11b Network [YES][no]:

Enable 802.11a Network [YES][no]:

Enable 802.11g Network [YES][no]:

Enable Auto-RF [YES][no]:

Configure a NTP server now? [YES][no]: no

Configure the system time now? [YES][no]: no

Warning! No AP will come up unless the time is set.

Please see documentation for more details.

Would you like to configure IPv6 parameters[YES][no]: no

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes



2.2 安装MS域 Security

安装 Windows AD 域服务 - 1

- 添加角色



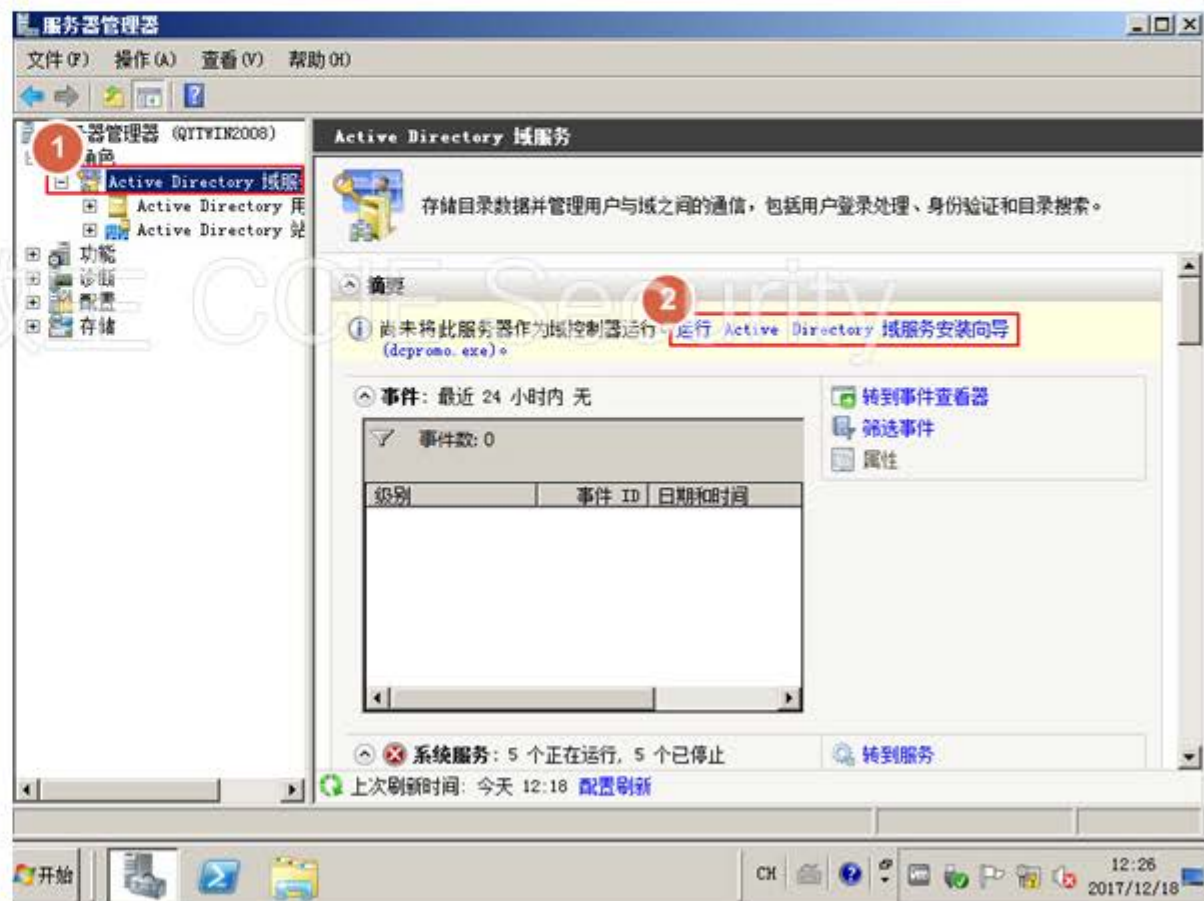
安装 Windows AD 域服务 - 2

- 勾选 Active Directory 域服务



安装 Windows AD 域服务 - 3

- 安装



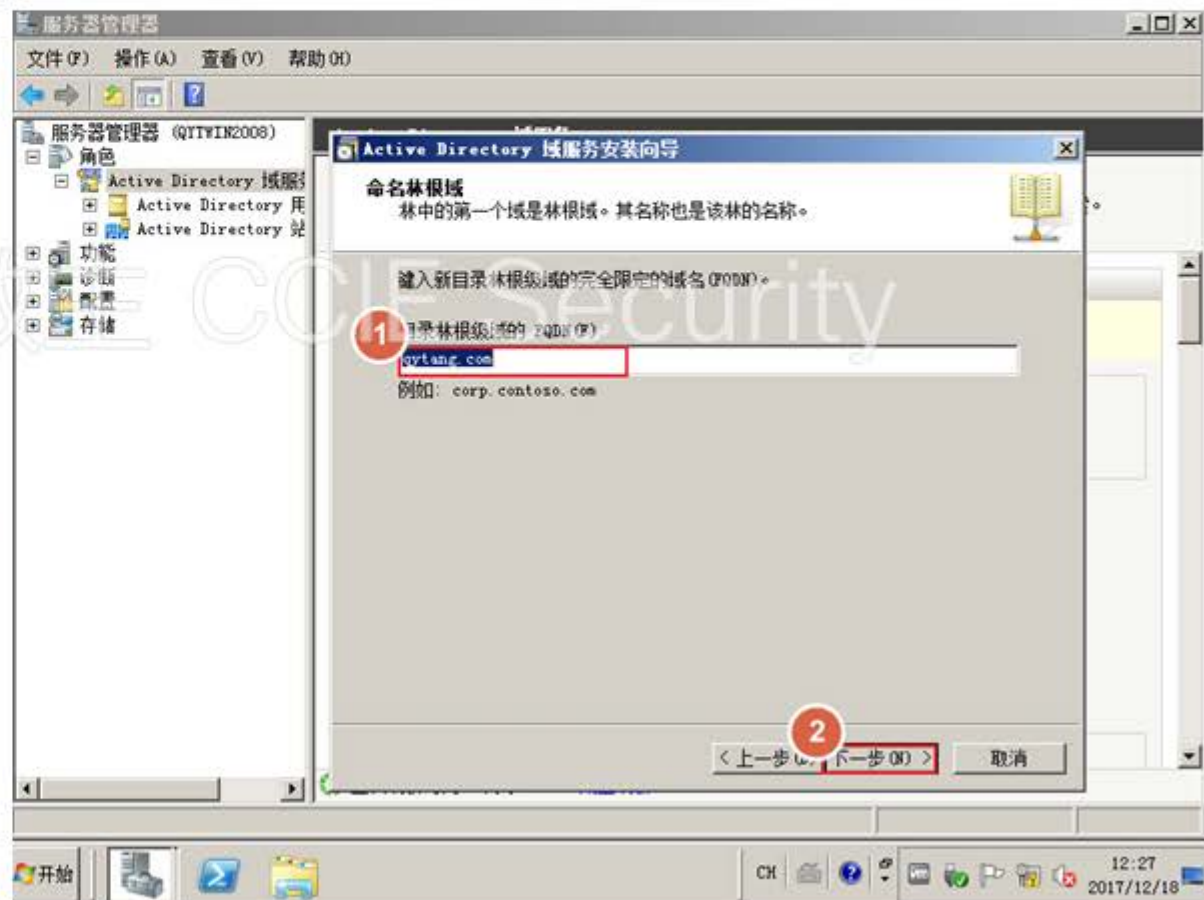
安装 Windows AD 域服务 - 4

- 使用高级模式安装



安装 Windows AD 域服务 - 5

- 新建域



安装 Windows AD 域服务 - 6

- 设置域 NetBIOS 名称



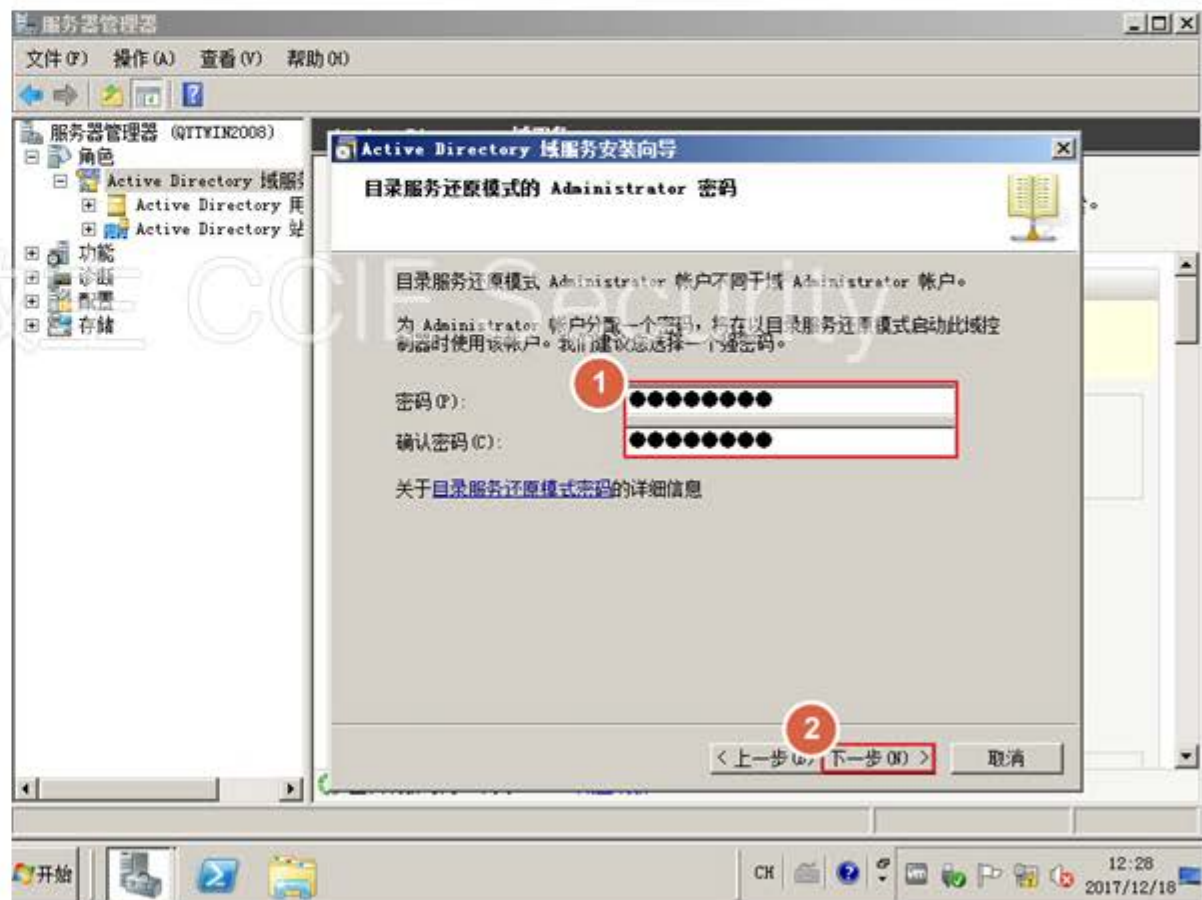
安装 Windows AD 域服务 - 7

- 新建 DNS 服务器



安装 Windows AD 域服务 - 8

- 设置 DNS 服务器参数



安装 Windows AD 域服务 - 9

- 完成 DNS 服务器安装





2.3 安装MS证书服务器

安装 AD 域证书服务 - 1

- 添加角色



安装 AD 域证书服务 - 2

- 安装 Active Directory 证书服务



安装 AD 域证书服务 - 3

- 勾选 证书颁发机构, 证书颁发机构 Web 注册



安装 AD 域证书服务 - 4

- 使用默认参数继续安装



安装 AD 域证书服务 - 5

- 使用默认参数继续安装



安装 AD 域证书服务 - 6

- 使用默认参数继续安装



安装 AD 域证书服务 - 7

- 使用默认参数继续安装



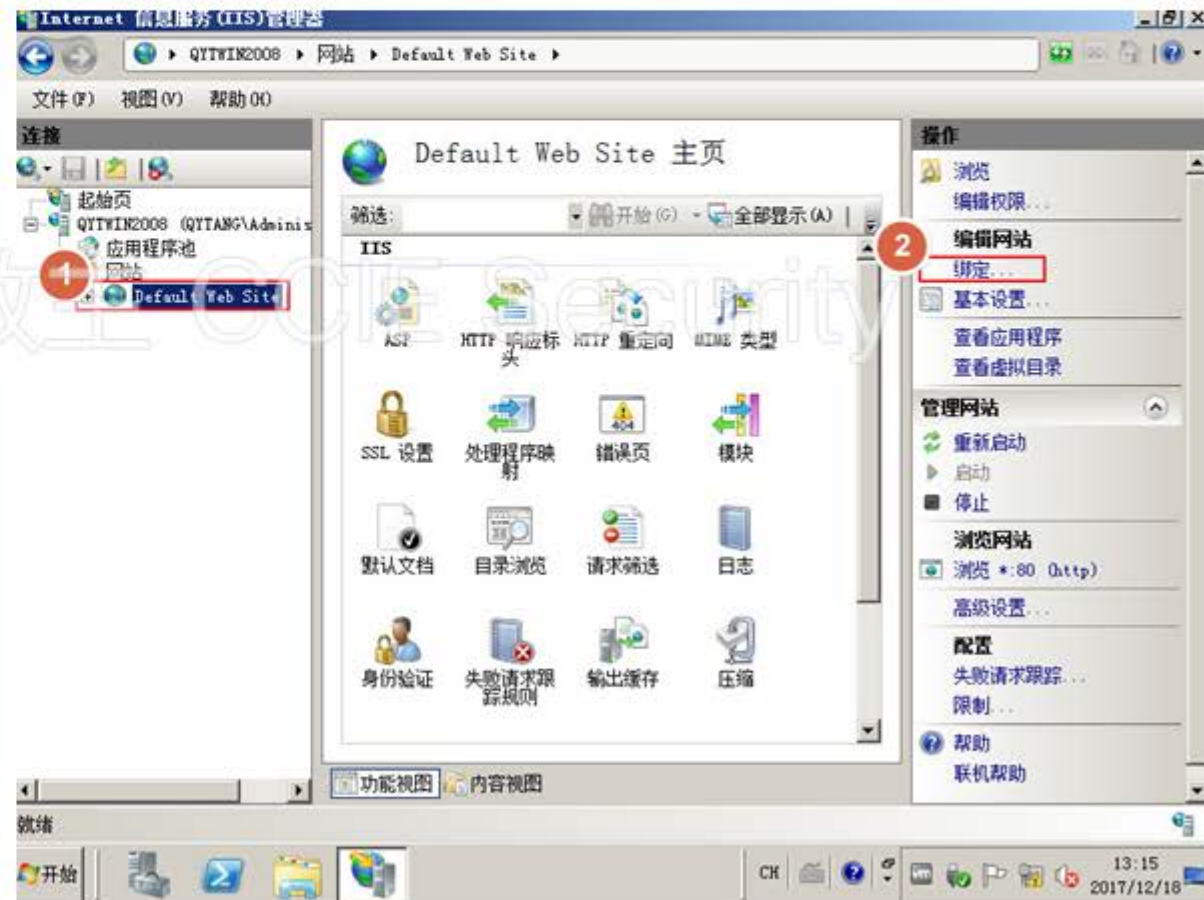
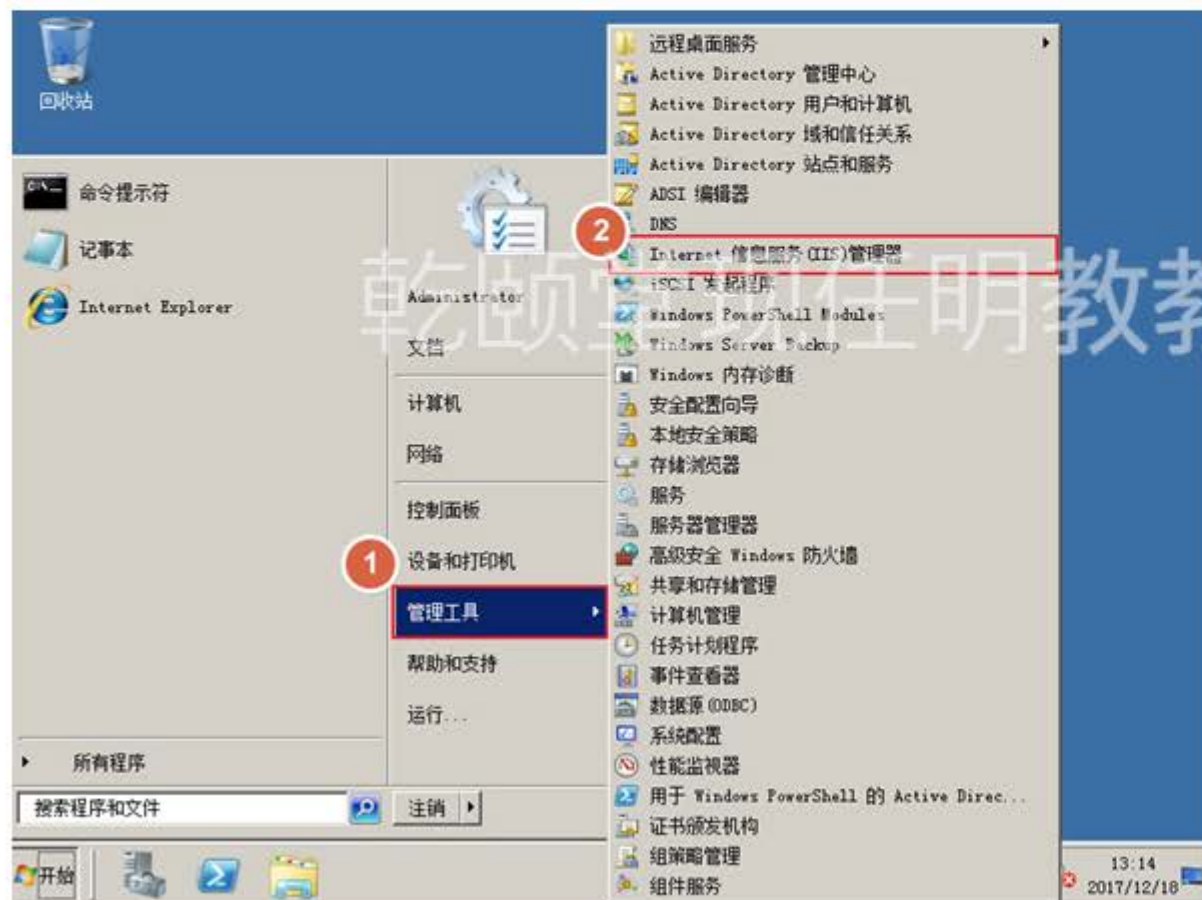
安装 AD 域证书服务 - 8

- 完成安装



绑定 HTTPS 证书 -1

- 打开「Internet 信息服务 (IIS) 管理器」，选择默认网站，点击绑定



绑定 HTTPS 证书 -2

- 为网站绑定 https 类型, 选择 SSL 证书

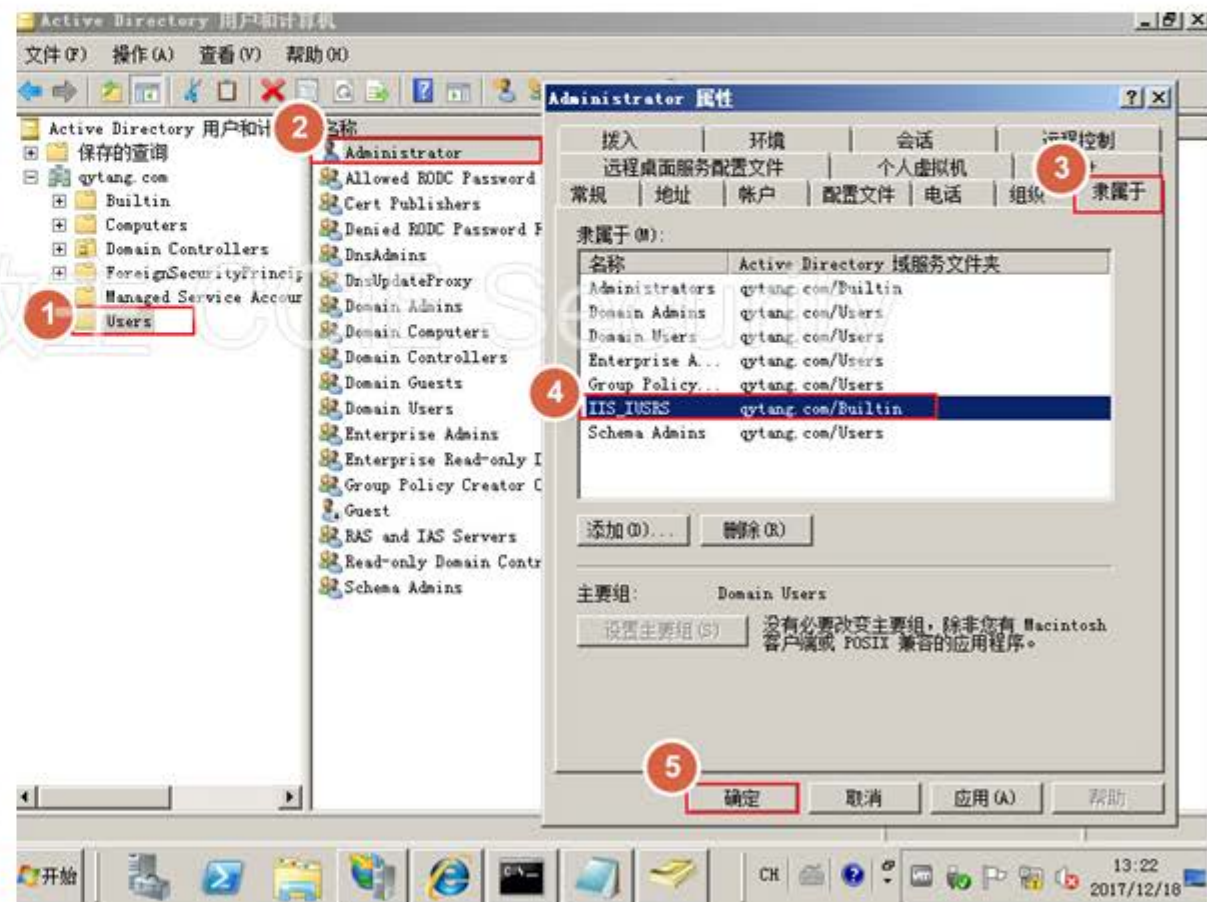




2.4 安装设备注册服务

将管理员用户添加到 IIS 用户组

- 将管理员用户添加到 IIS 用户组



安装设备注册服务 (NDS) - 1

- 在 Active Directory 证书服务器下添加角色服务，选择 网络设备注册服务



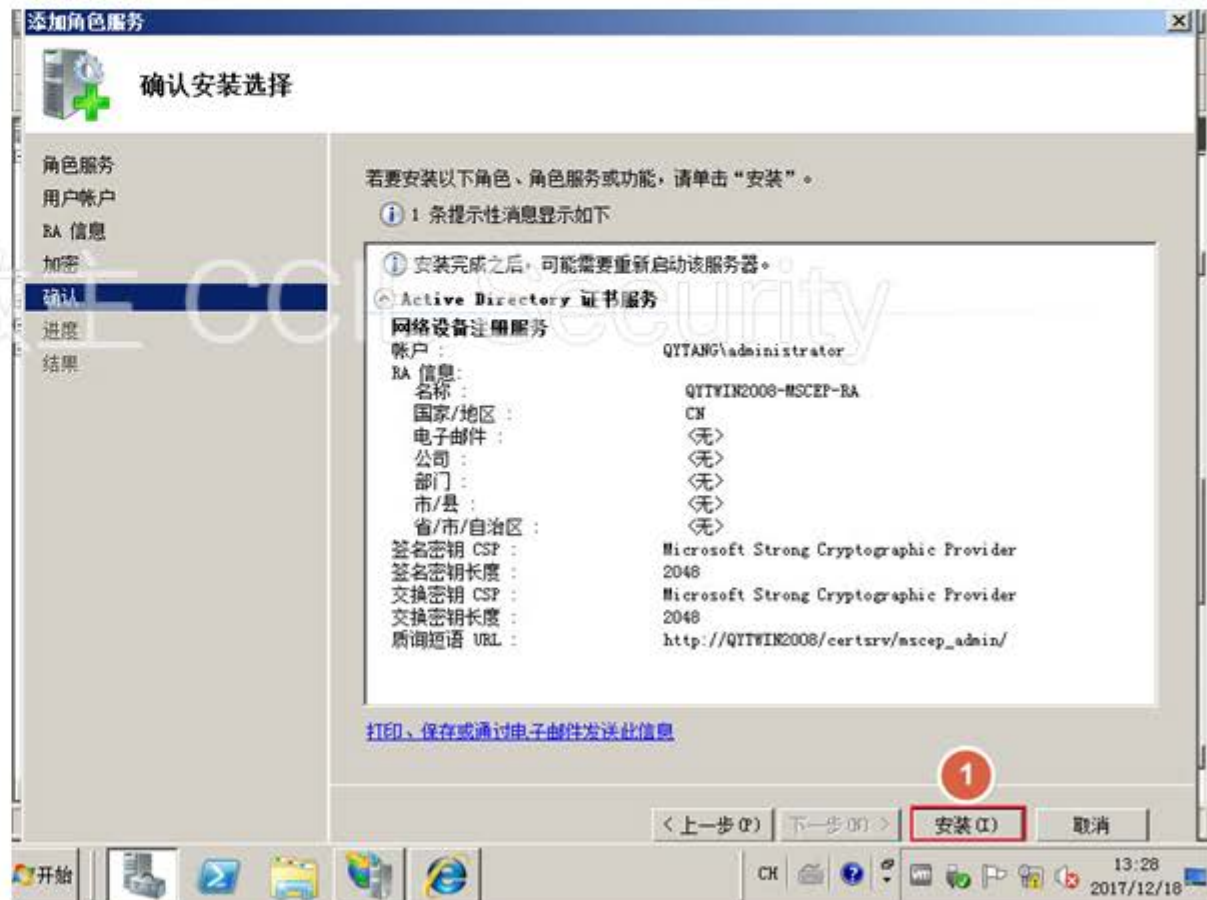
安装设备注册服务 (NDS) - 2

- 指定管理员账户



安装设备注册服务 (NDS) - 3

- 使用默认参数安装



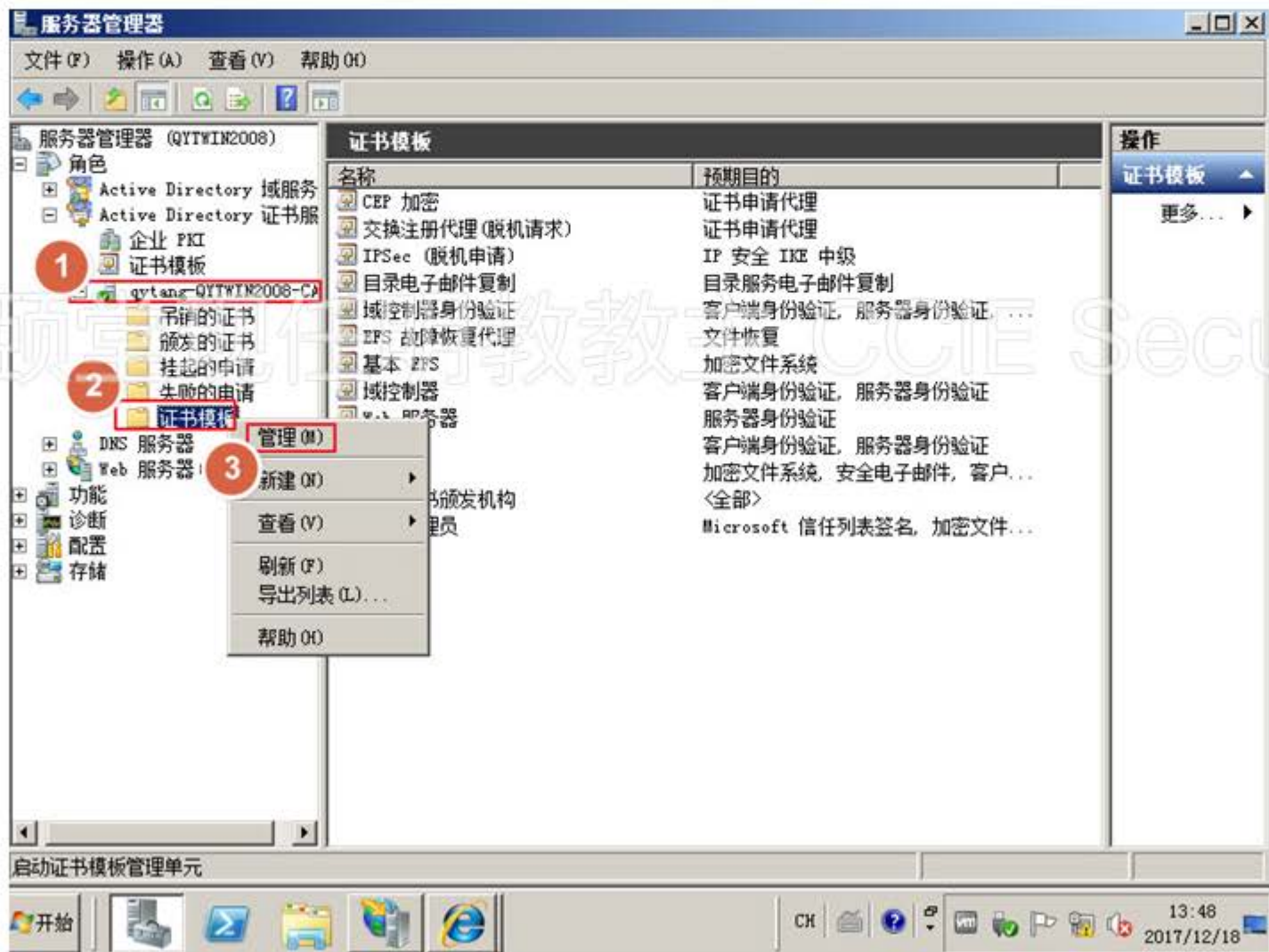
查看设备注册服务 (MSCEP) 正常运行

- 打开 https://qytwm2008.qytang.com/certsrv/mscep_admin 查看服务是否正常运行



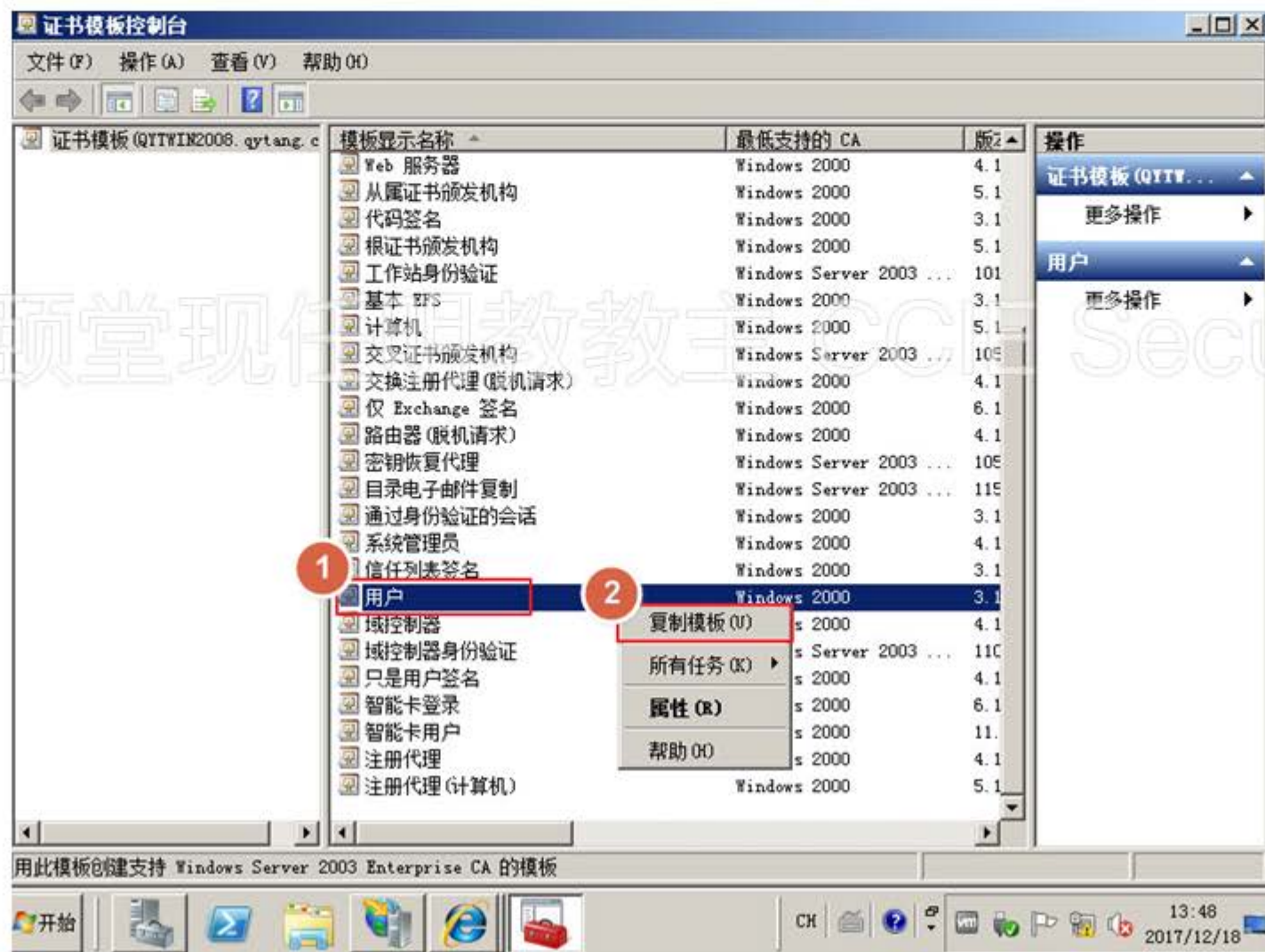
创建 BYOD 证书模版 -1

- 管理证书模板



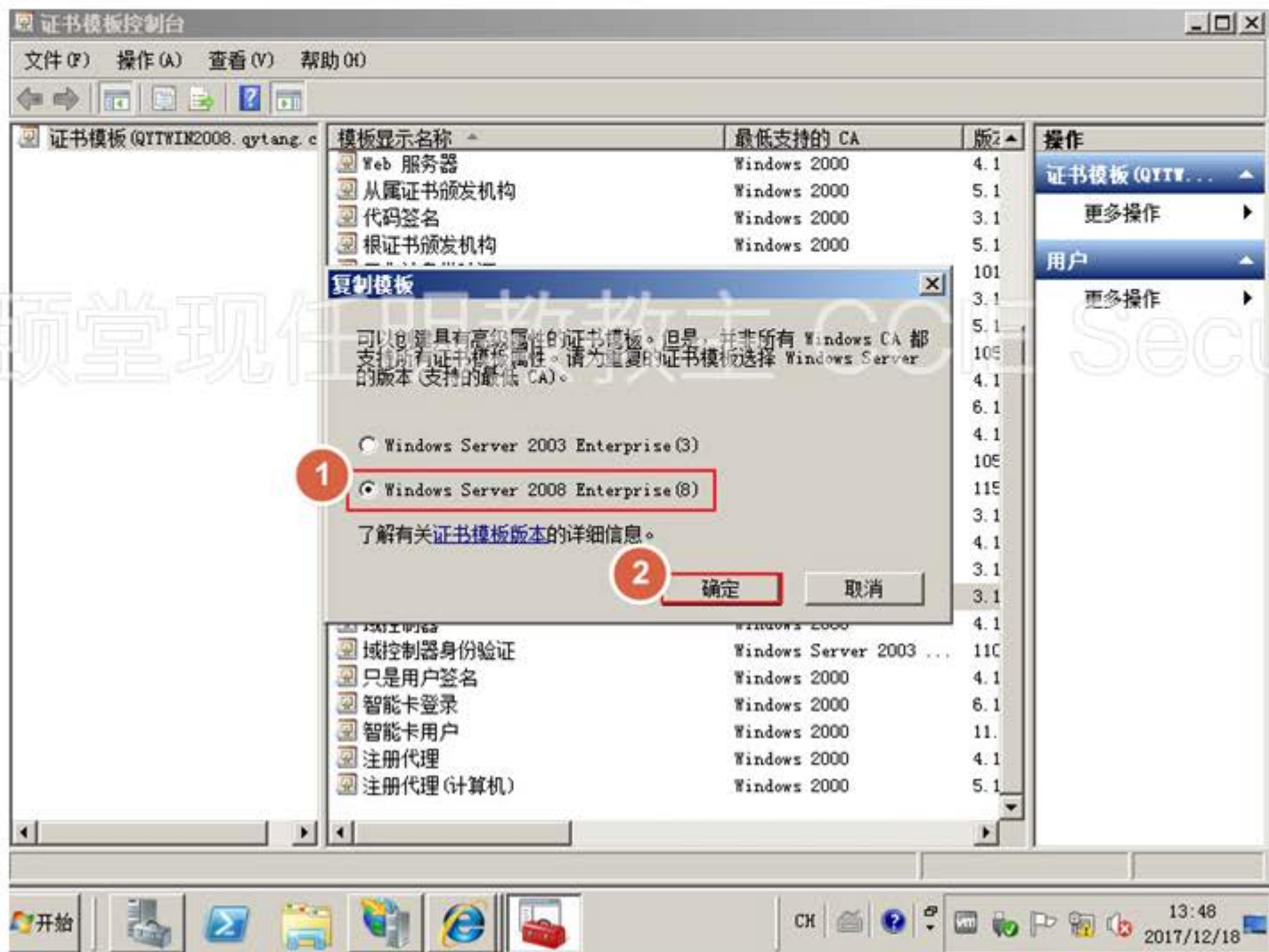
创建 BYOD 证书模版 -2

- 复制「用户」模板



创建 BYOD 证书模版 -3

- 确定



创建 BYOD 证书模版 -4

- 修改 BYOD 模板参数

新模板的属性

服务器 | 发布要求 | 取代模板 | 扩展 | 安全
常规 | 请求处理 | 加密 | 使用者名称

1 板显示名称 (E):
USER_BYOD

最低支持的 CA: Windows Server 2008 Enterprise

模板名 (T):
USER_BYOD

有效期 (V): 1 年 | 续订期 (R): 6 周

在 Active Directory 中发布证书 (P)
 如果 Active Directory 中有一个重复证书, 不要自动重新注册 (R)
 对于智能卡证书的自动续订, 如果无法创建新密钥, 请使用现有密钥 (P)

确定 取消 应用 (A) 帮助

新模板的属性

服务器 | 发布要求 | 取代模板 | 扩展 | 安全
常规 | 1 请求处理 | 加密 | 使用者名称

目的 (P): 签名和加密

删除吊销的或过期的证书 (不存档) (O)
 包括使用者允许的对称算法 (X)
 把使用者的加密私钥存档 (O)
 使用高级对称算法将密钥发送给 CA (S)

2 允许导出私钥 (O)

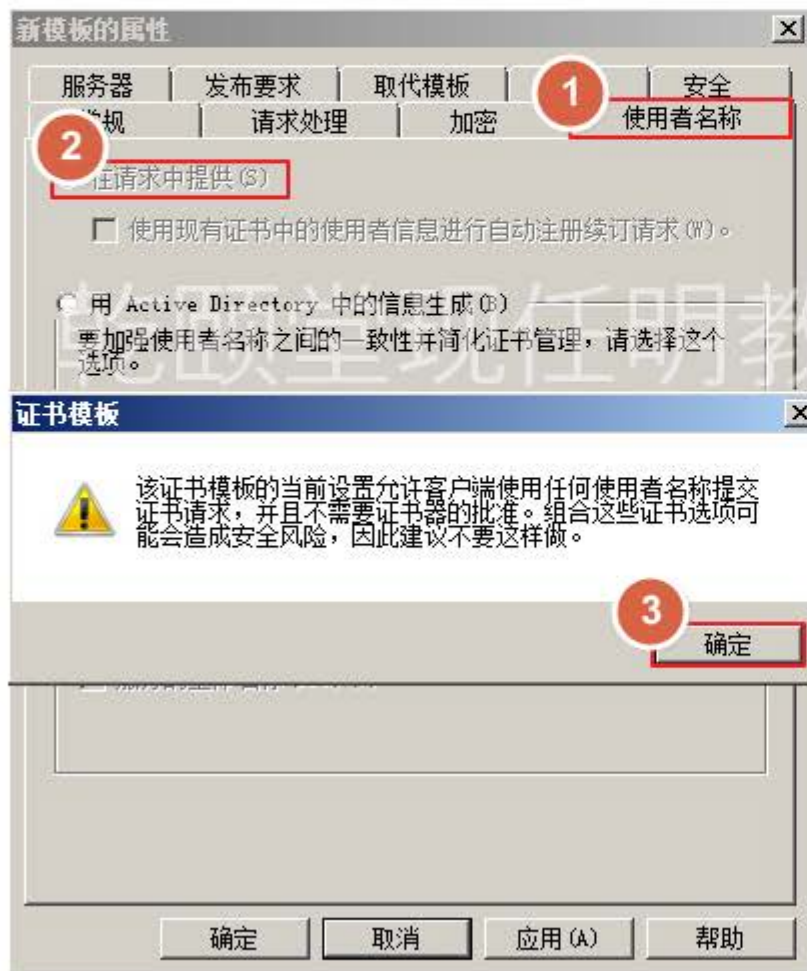
当使用者已经注册, 并且使用了与该证书相关的私钥, 执行以下操作:

注册证书使用者时无需用户输入 (E)
 注册时提示用户 (R)
 在私钥被使用的情况下, 注册时提示用户并要求用户输入 (U)

确定 取消 应用 (A) 帮助

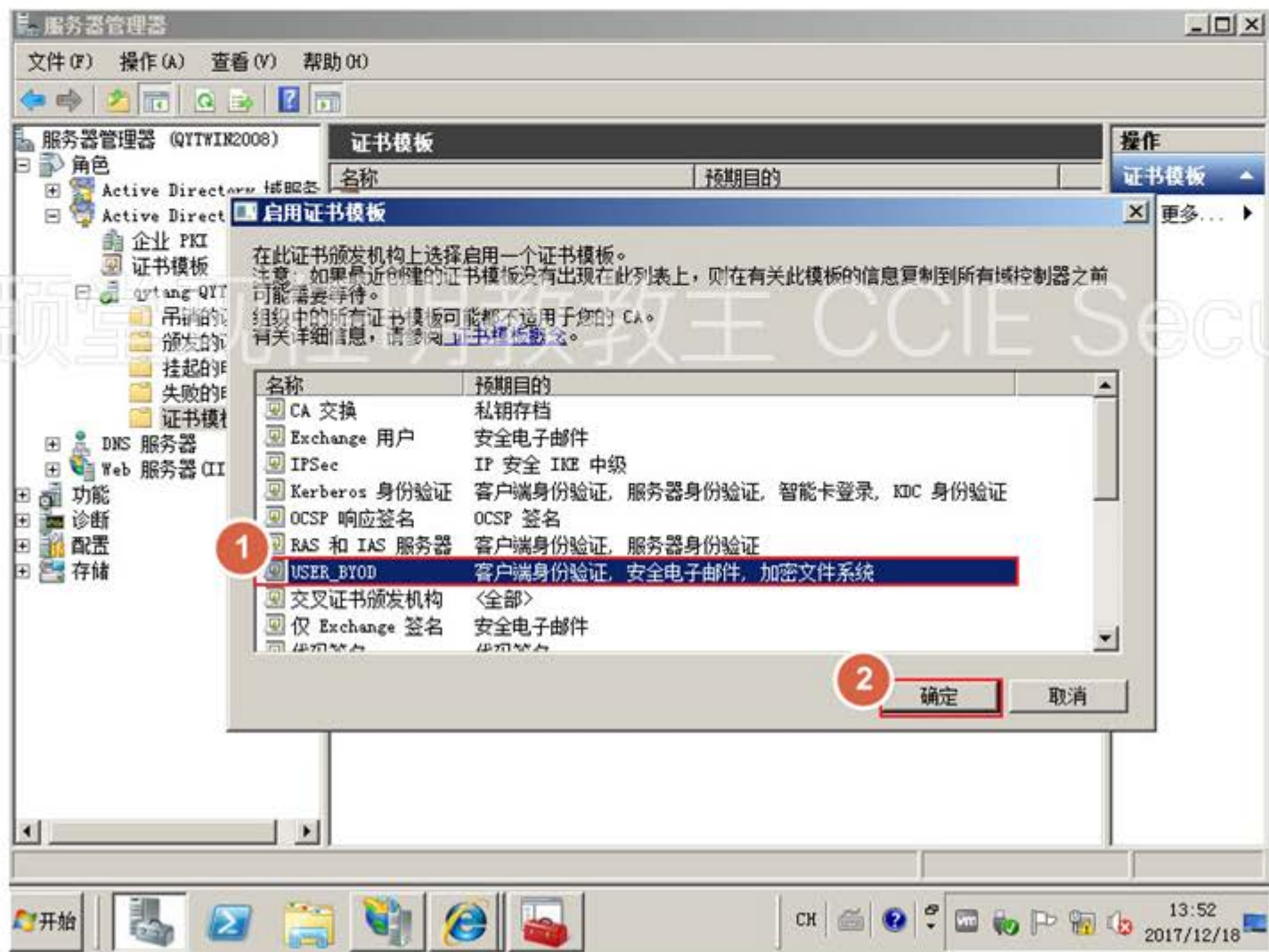
创建 BYOD 证书模版 -5

- 修改 BYOD 模板参数



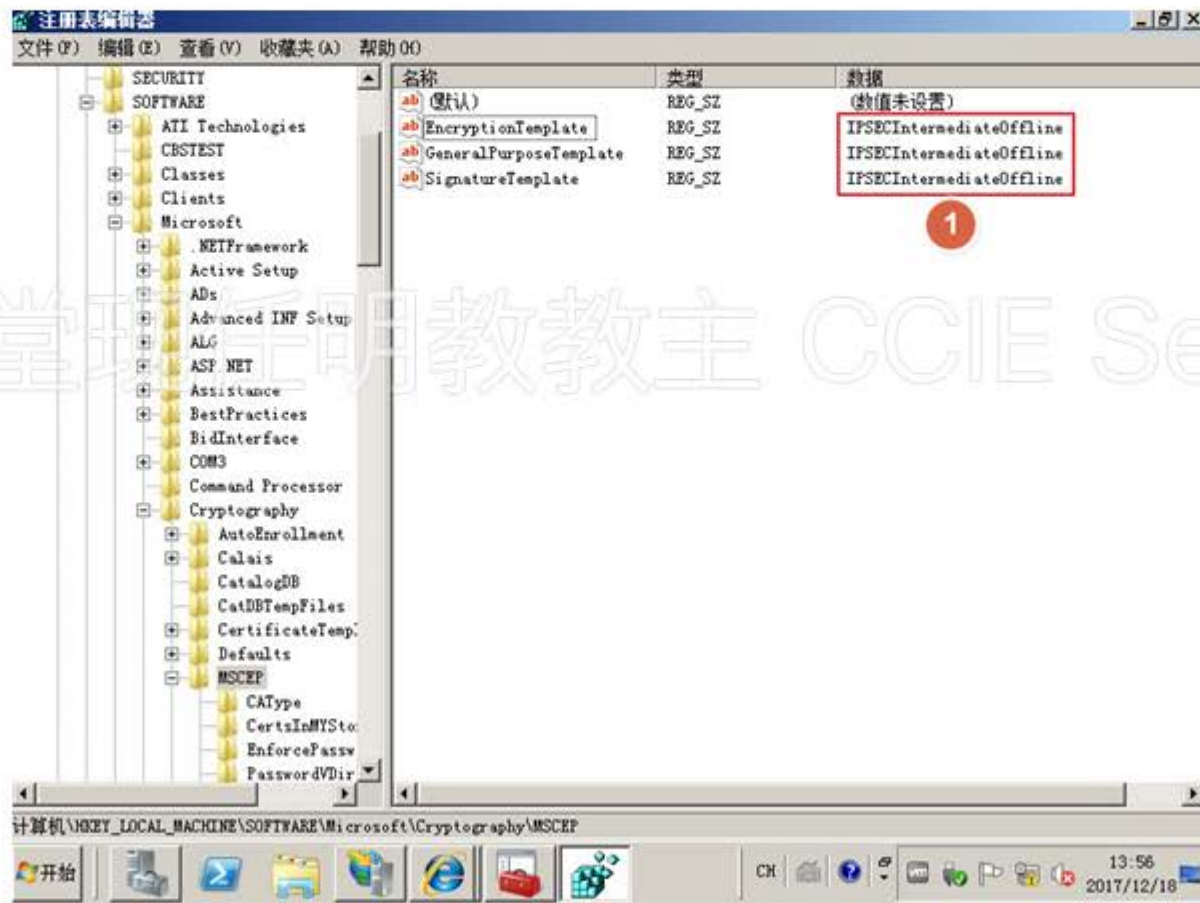
颁发 BYOD 证书模版 - 2

- 选择模板



修改 MSCEP 颁发的默认证书模板- 1

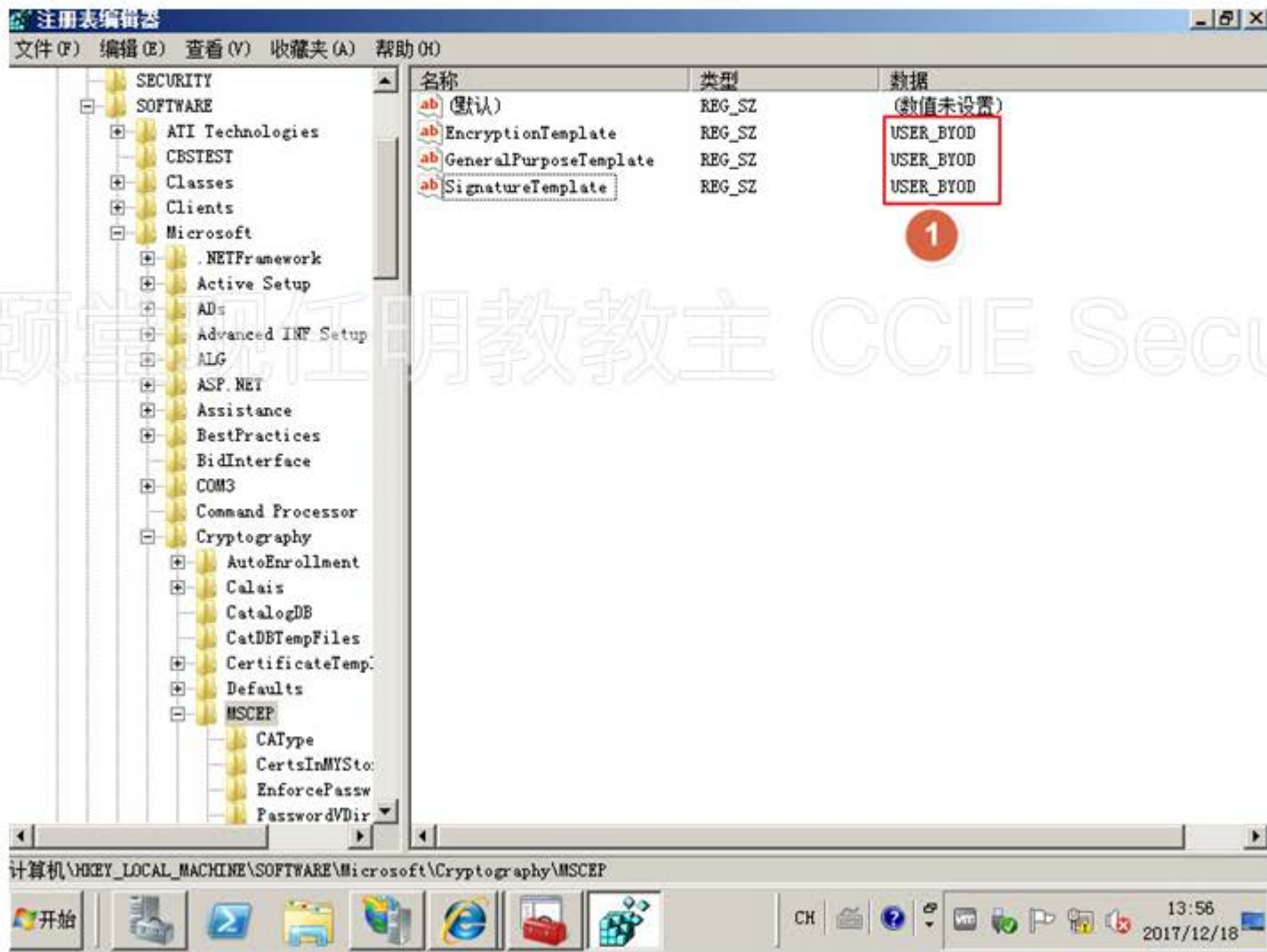
- 默认的 MSCEP 的颁发的模版是 IPSEC 离线证书申请的模版



cmd 命令“regedit”打开注册表，注册表的路径是：**HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP**

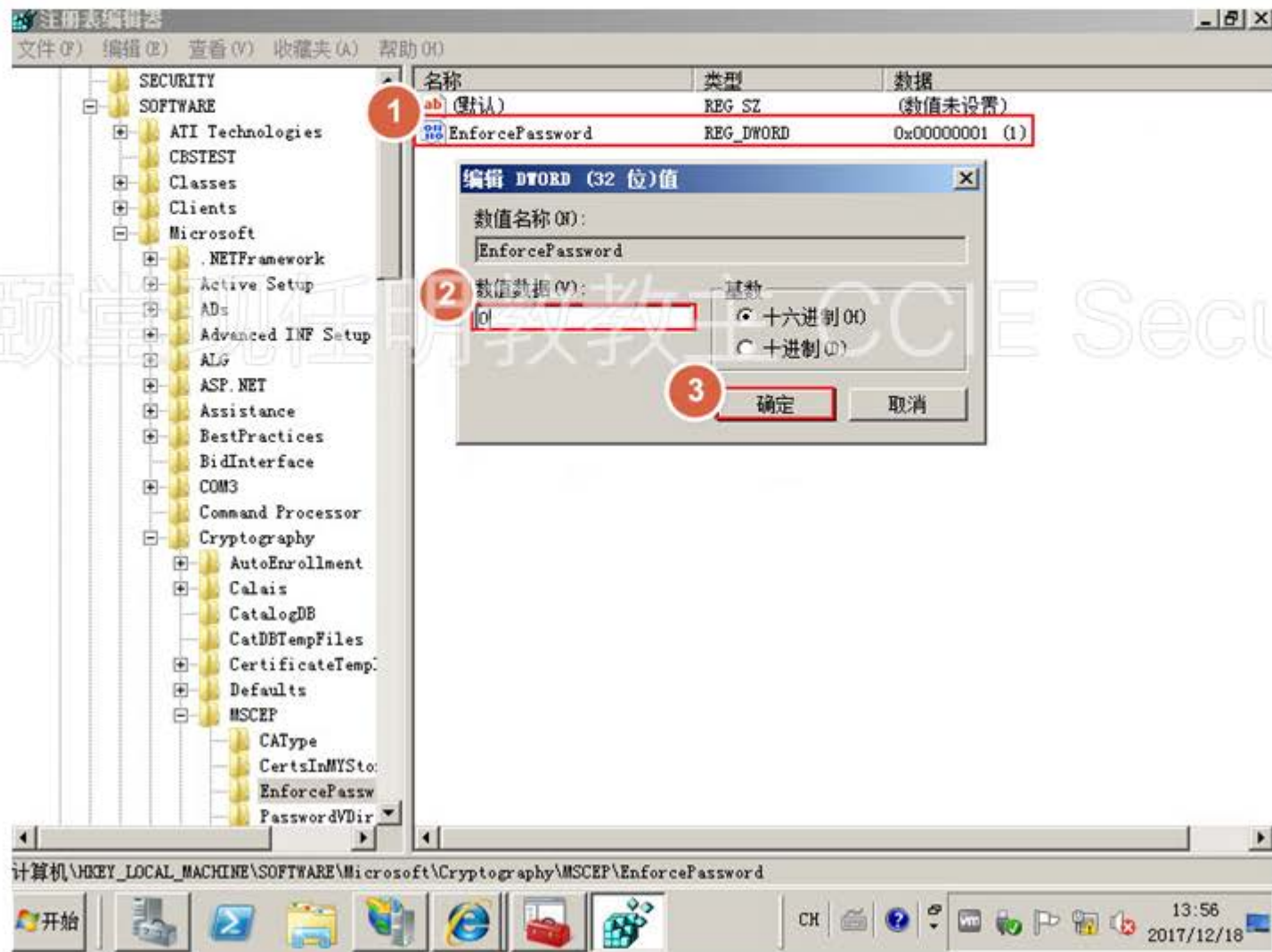
修改 MSCEP 颁发的默认证书模板- 1

- 修改颁发的证书模板



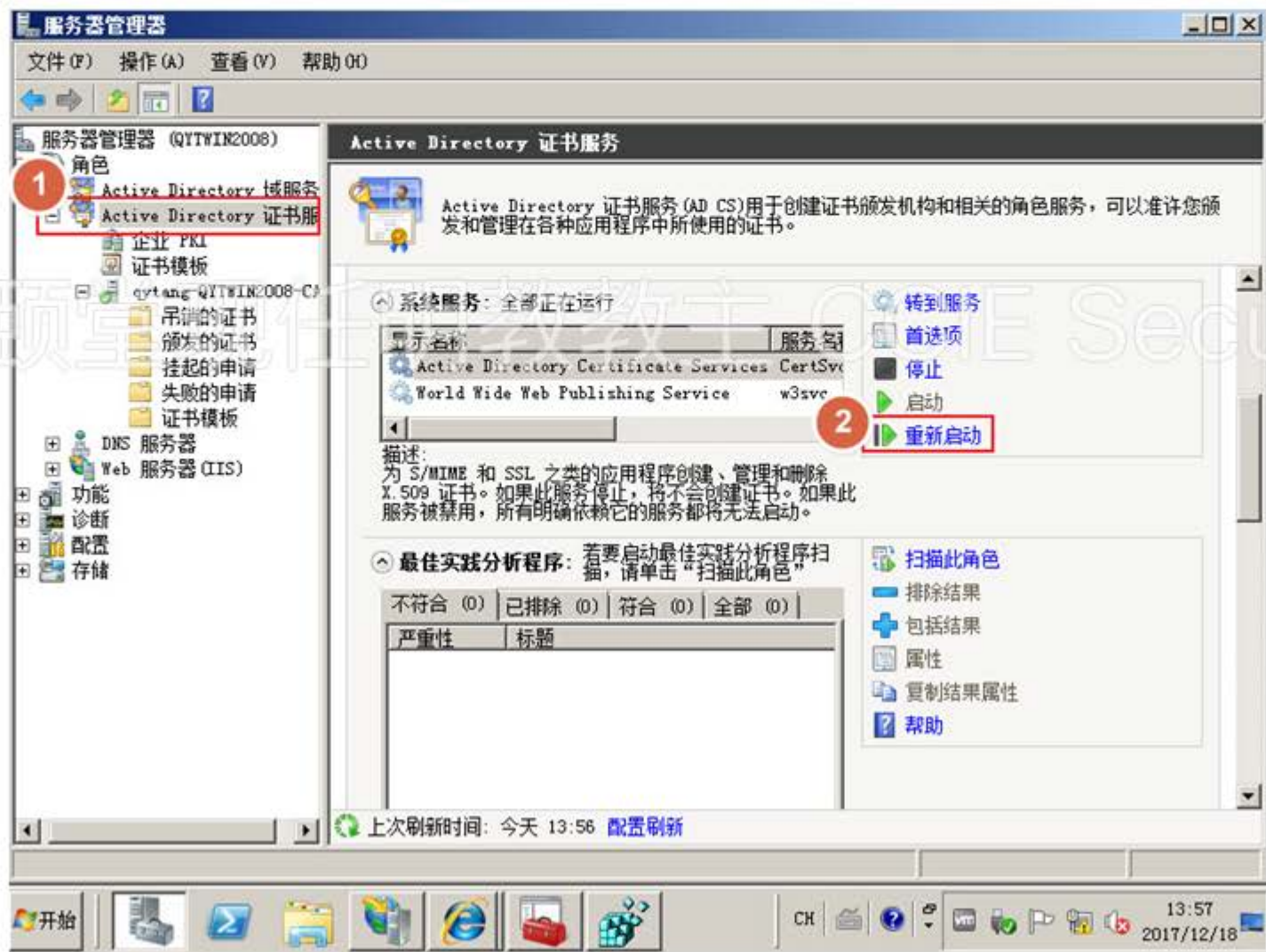
无需密码申请证书

- 颁发证书默认需要密码，这里修改为不需要密码，否则 ISE 无法为设备代理申请证书



重启服务激活策略

- 点击 Active Directory 证书服务，重新启动服务

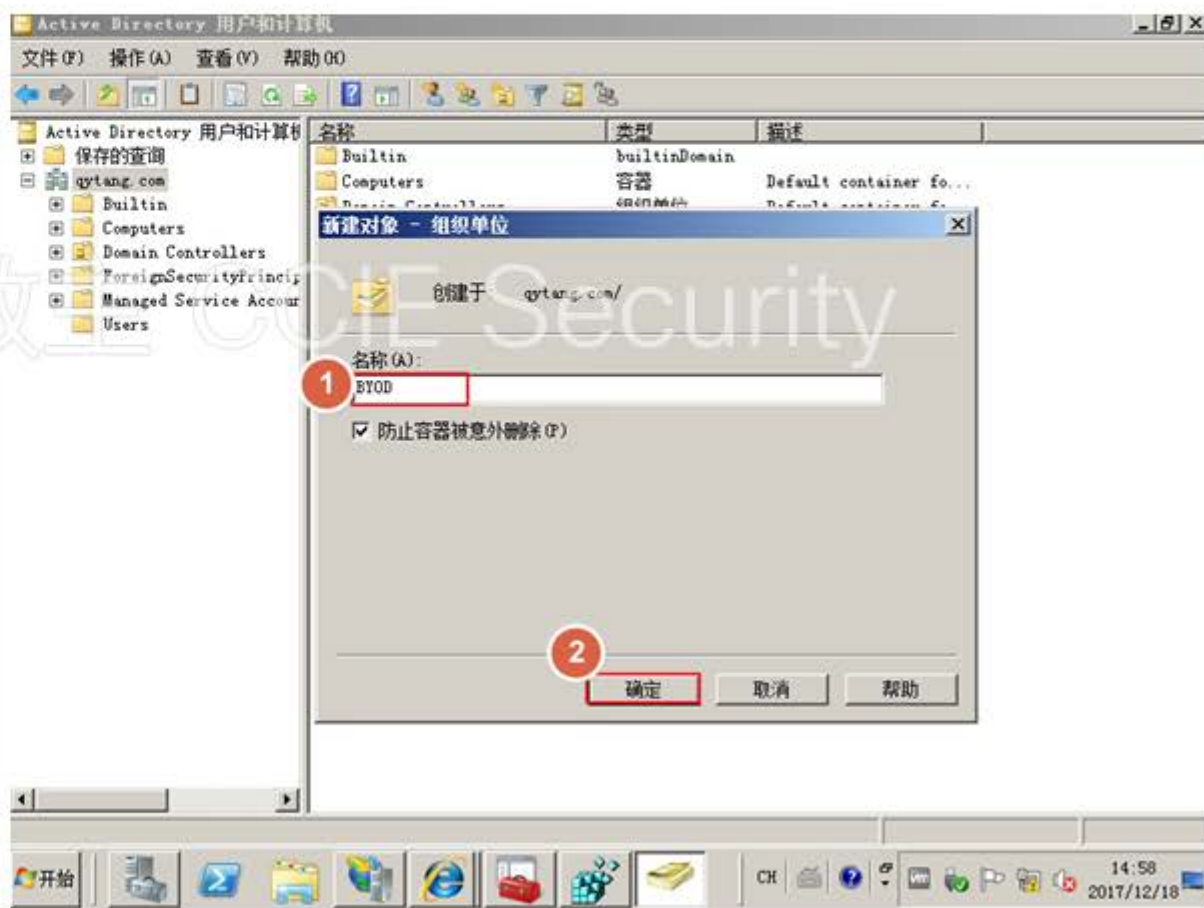
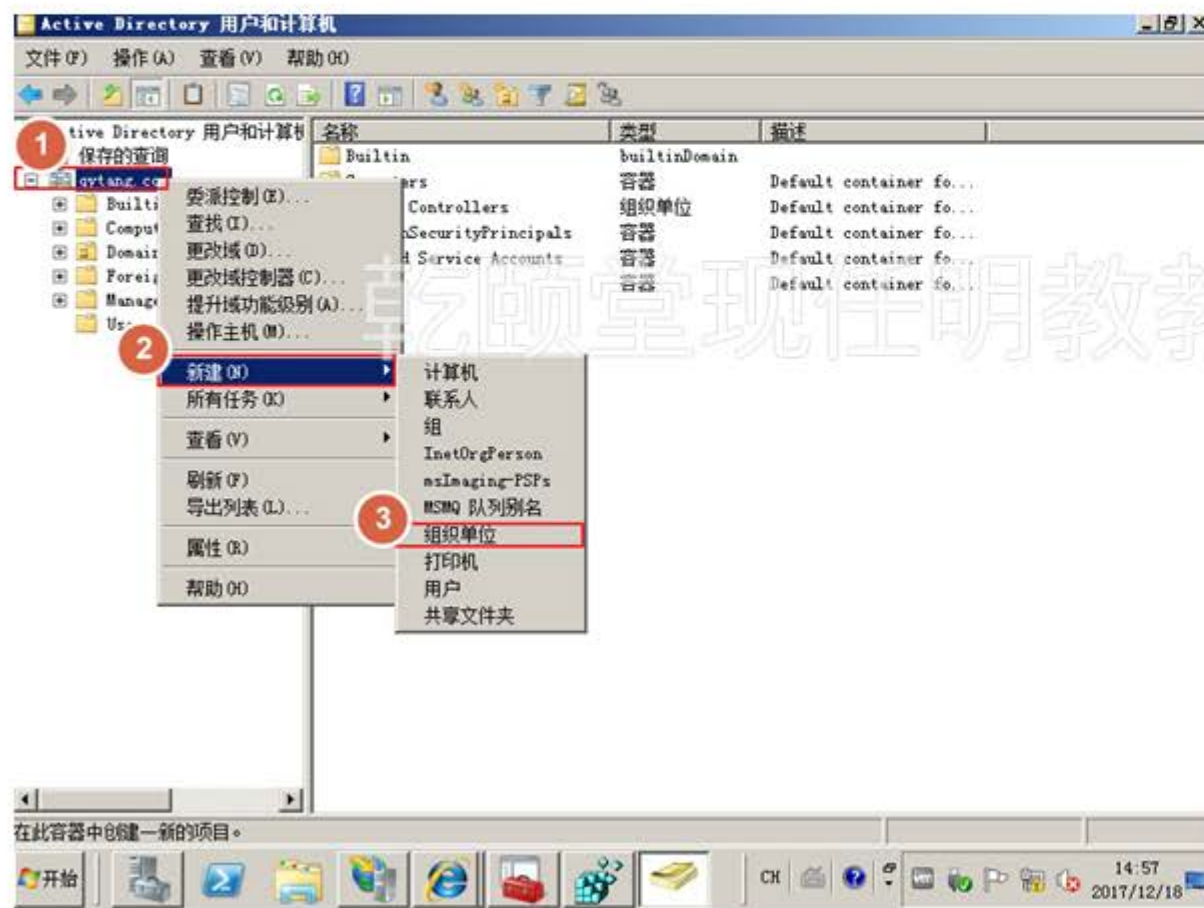




2.5 创建注册单位、组 and 用户

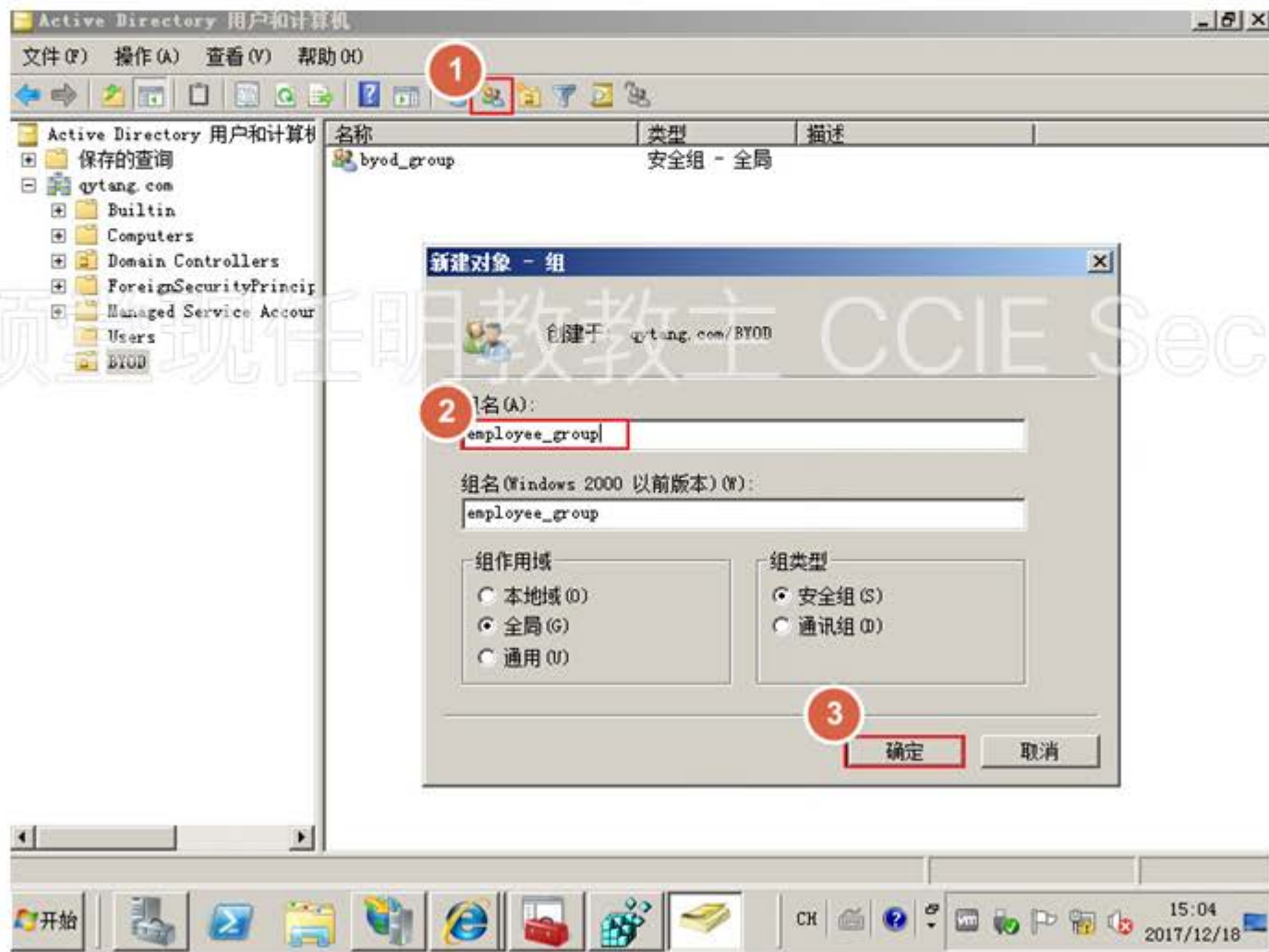
新建组织单位

- 在 qytang.com 下新建组织单位：BYOD



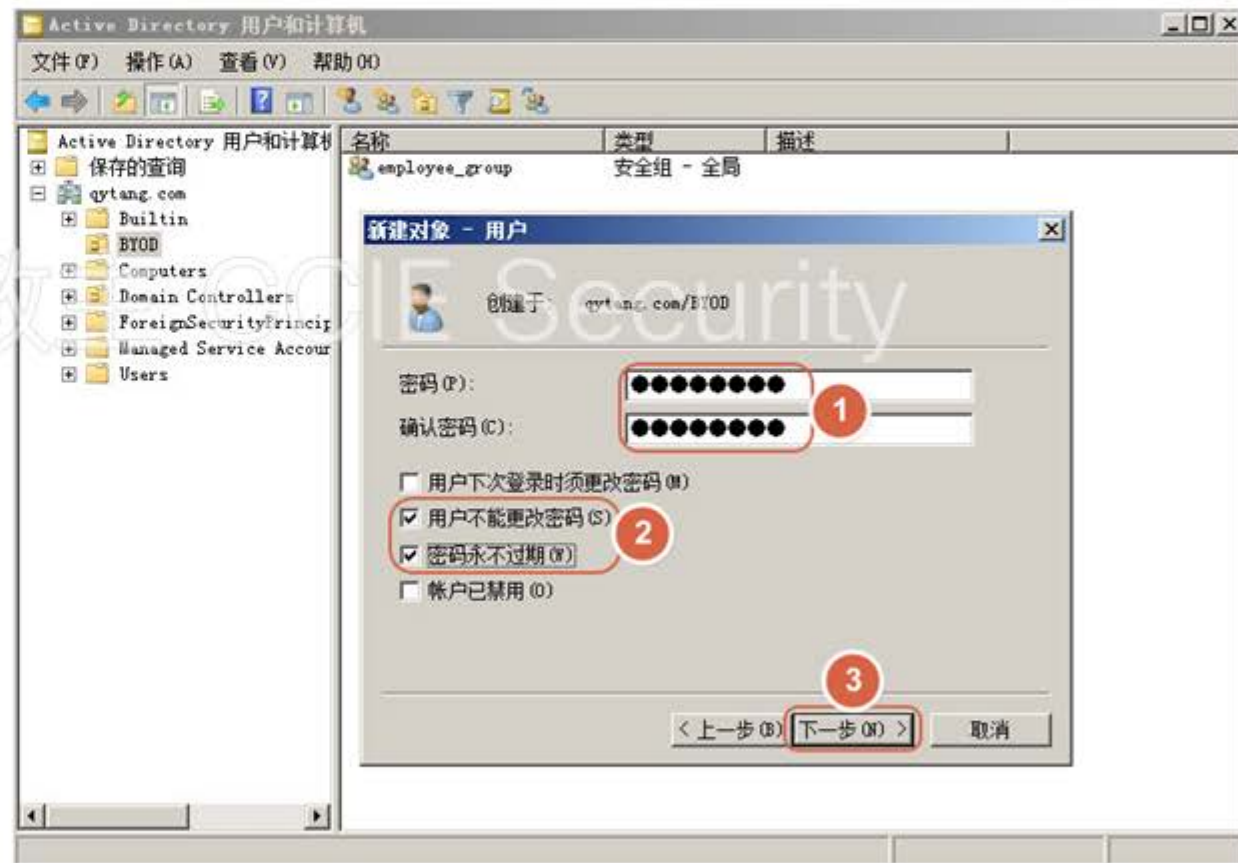
新建用户组

- 新建用户组employee_group



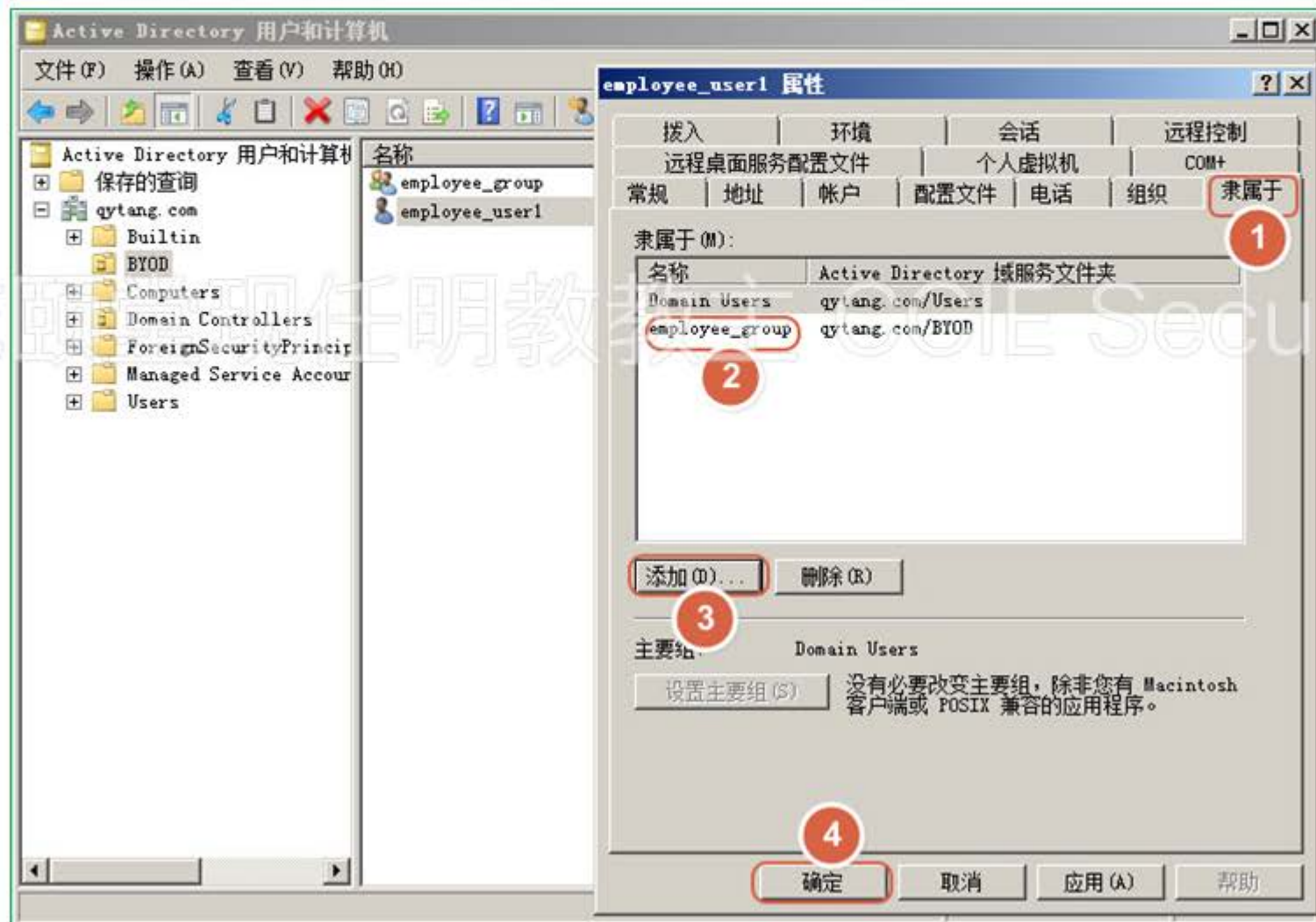
新建用户 - 1

- 新建用户 employee_user1, 修改密码策略



新建用户 - 2

- 用户 employee_user1 隶属于 employee_group





3. ISE基本证书与域操作

3.1 ISE申请证书

乾颐堂 3.2 添加SCEP证书服务器 ISE Security

3.3 创建BYOD证书申请模板

3.4 Native Supplicant Profile

3.5 Client Provisioning策略

3.6 ISE集成MS域



3.1 ISE 申请证书

ISE 添加根证书 - 1

- 进入证书申请页面，下载根证书



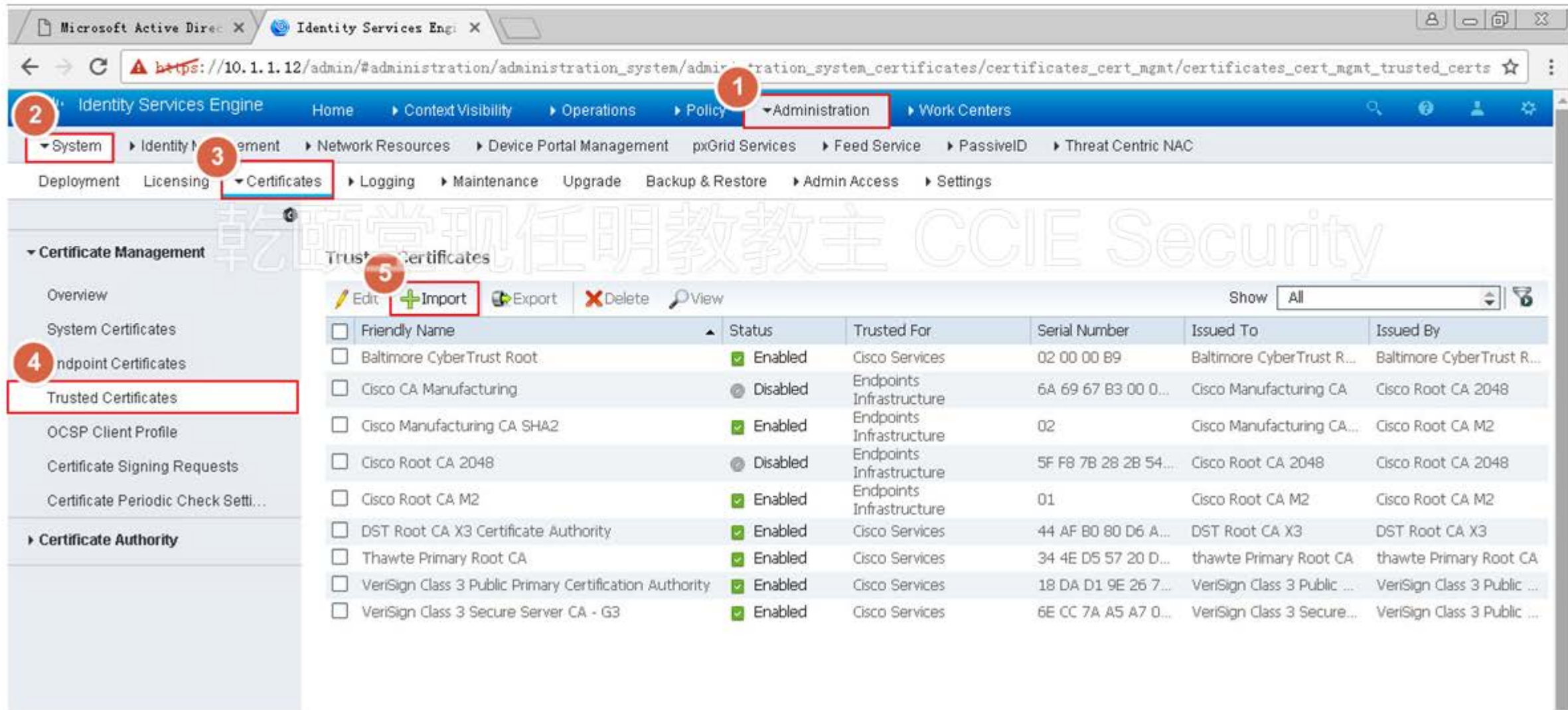
ISE 添加根证书 - 2

- 下载 CA 证书, 保存

The screenshot shows a web browser window with the address bar containing `https://10.1.1.10/certsrv/certcarc.asp`. The page title is "Microsoft Active Directory 证书服务 -- qytang-QYTWIN2008-CA". The main heading is "下载 CA 证书、证书链或 CRL". Below this, there is a paragraph: "若要信任从此证书颁发机构颁发的证书, 请安装此 CA 证书。" and another: "要下载一个 CA 证书、证书链或 CRL, 选择证书和编码方法。". Under the heading "CA 证书:", there is a dropdown menu with "当前 [qytang-QYTWIN2008-CA]" selected. Under the heading "编码方法:", there are two radio buttons: "DER" (selected) and "Base 64". At the bottom, there are several links: "安装 CA 证书" (with a red circle containing the number 1), "下载 CA 证书", "下载 CA 证书链", "下载最新的基 CRL", and "下载最新的增量 CRL". A large, semi-transparent watermark "软研堂现任明教教主 CCIE Security" is overlaid on the page content.

ISE 添加根证书 - 3

- ISE 导入根证书



The screenshot shows the ISE Administration console interface. The navigation path is: Administration > System > Certificates > Trusted Certificates. The 'Import' button is highlighted in the toolbar. The table below lists the current trusted certificates.

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By
Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust R...	Baltimore CyberTrust R...
Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 0...	Cisco Manufacturing CA	Cisco Root CA 2048
Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA...	Cisco Root CA M2
Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54...	Cisco Root CA 2048	Cisco Root CA 2048
Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2
DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A...	DST Root CA X3	DST Root CA X3
Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D...	thawte Primary Root CA	thawte Primary Root CA
VeriSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7...	VeriSign Class 3 Public ...	VeriSign Class 3 Public ...
VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 0...	VeriSign Class 3 Secure...	VeriSign Class 3 Public ...

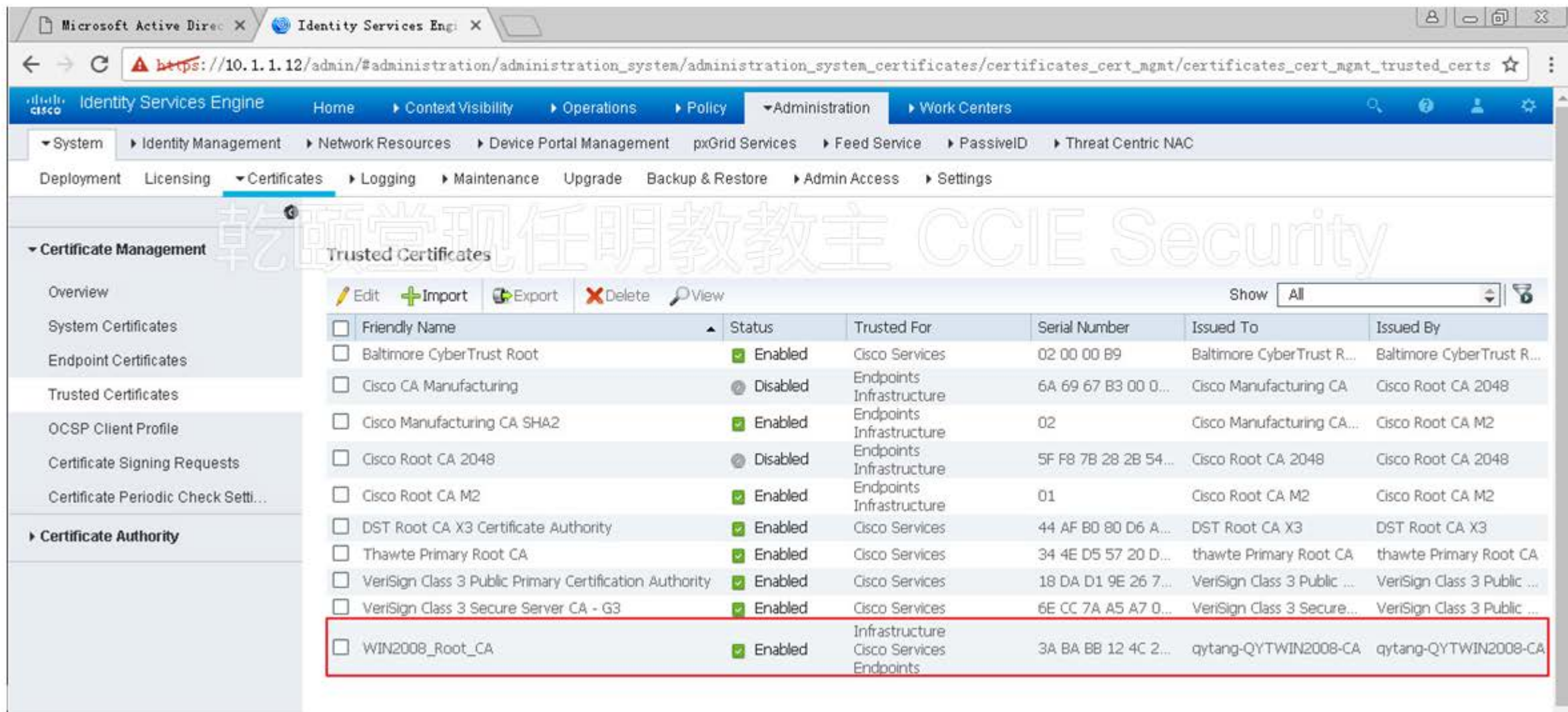
ISE 添加根证书 - 4

- 选择证书文件导入

The screenshot displays the Cisco Identity Services Engine (ISE) administration console. The browser address bar shows the URL: `https://10.1.1.12/admin/#administration/administration_system/administration_system_certificates/certificates_cert_mgmt/certificates_cert_mgmt_trusted_certs`. The navigation menu on the left includes "Certificate Management" and "Certificate Authority". The main content area shows the "Import a new Certificate into the Certificate Store" form. The form fields are: "Certificate File" (selected as "certnew.cer"), "Friendly Name" (set to "WIN2008_Root_CA"), "Trusted For" (with three checked options: "Trust for authentication within ISE", "Trust for client authentication and Syslog", and "Trust for authentication of Cisco Services"), and "Description" (empty). A "Submit" button is visible at the bottom. A warning dialog box on the right states: "This Certificate has a signature that uses the SHA-1 hashing algorithm and is considered less secure. Are you sure you want to import this certificate?" with "Yes" and "No" buttons.

查看 ISE 添加的根证书

- 查看导入的根证书信息

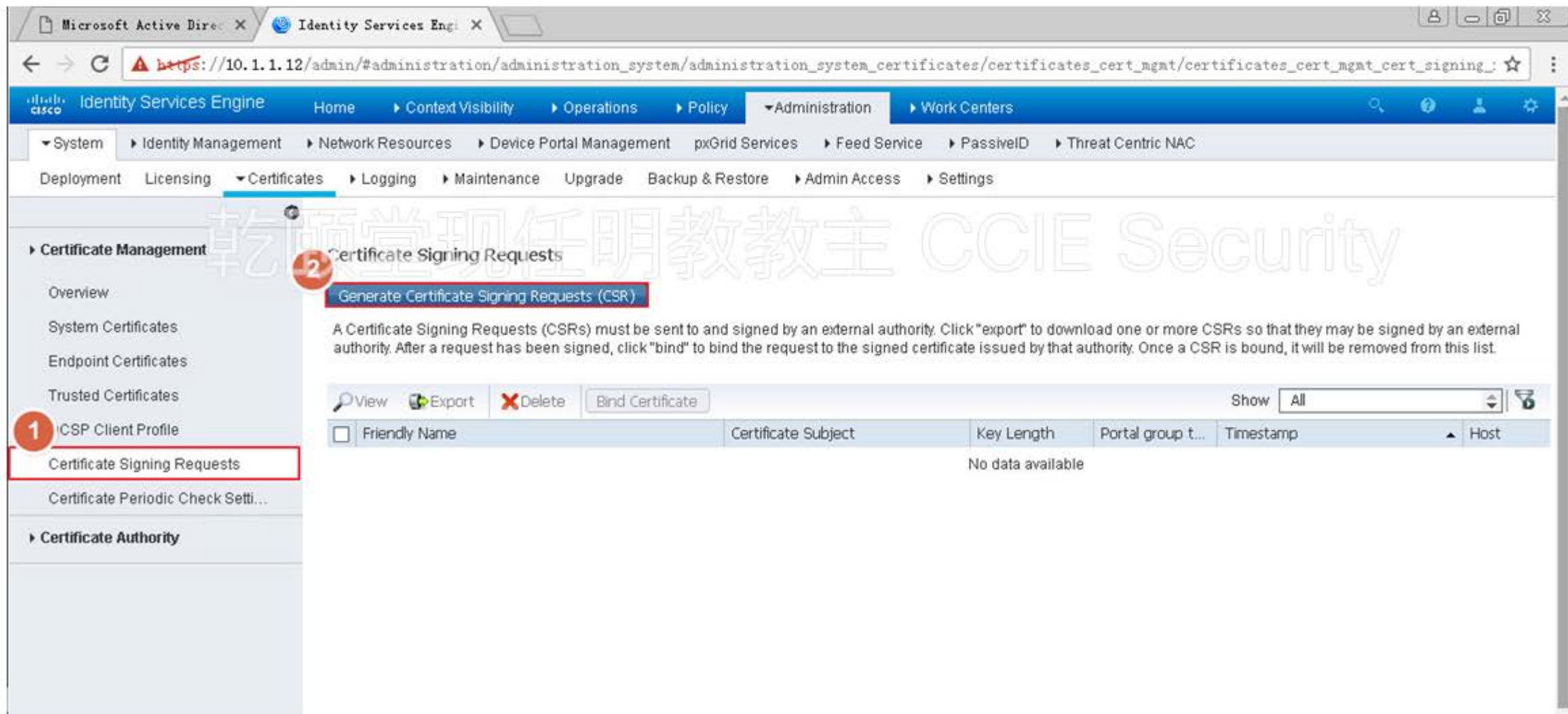


The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu is set to Administration > Work Centers > Certificates. The 'Trusted Certificates' page is displayed, showing a table of certificates. The 'WIN2008_Root_CA' certificate is highlighted with a red box.

<input type="checkbox"/>	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By
<input type="checkbox"/>	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust R...	Baltimore CyberTrust R...
<input type="checkbox"/>	Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 0...	Cisco Manufacturing CA	Cisco Root CA 2048
<input type="checkbox"/>	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA...	Cisco Root CA M2
<input type="checkbox"/>	Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54...	Cisco Root CA 2048	Cisco Root CA 2048
<input type="checkbox"/>	Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2
<input type="checkbox"/>	DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A...	DST Root CA X3	DST Root CA X3
<input type="checkbox"/>	Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D...	thawte Primary Root CA	thawte Primary Root CA
<input type="checkbox"/>	VeriSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7...	VeriSign Class 3 Public ...	VeriSign Class 3 Public ...
<input type="checkbox"/>	VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 0...	VeriSign Class 3 Secure...	VeriSign Class 3 Public ...
<input type="checkbox"/>	WIN2008_Root_CA	Enabled	Infrastructure Cisco Services Endpoints	3A BA BB 12 4C 2...	qytang-QYTWIN2008-CA	qytang-QYTWIN2008-CA

ISE 生成 CSR 文件 -1

- ISE 生成 CSR 文件，准备用于申请设备证书



Microsoft Active Dire... Identity Services Engi...
https://10.1.1.12/admin/#administration/administration_system/administration_system_certificates/certificates_cert_mgmt/certificates_cert_mgmt_cert_signing_

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Passiveld Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

- Overview
- System Certificates
- Endpoint Certificates
- Trusted Certificates
- 1 CSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Setti...

Certificate Authority

2 Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

View Export Delete Bind Certificate Show All

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal group t...	Timestamp	Host
No data available						

ISE 生成 CSR 文件 -2

- 填写主题信息后产生 CSR 文件，并导出 CSR 文件

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The navigation pane on the left includes 'Certificate Management' and 'Certificate Authority'. The main content area displays the 'Certificates' section for the 'QYTISE2-Master' node. The 'Subject' form is filled with the following information:

- Common Name (CN): \$FQDN\$
- Organizational Unit (OU): BYOD
- Organization (O):
- City (L):
- State (ST):
- Country (C):
- Subject Alternative Name (SAN):
- * Key type: RSA
- * Key Length: 2048
- * Digest to Sign With: SHA-256
- Certificate Policies:

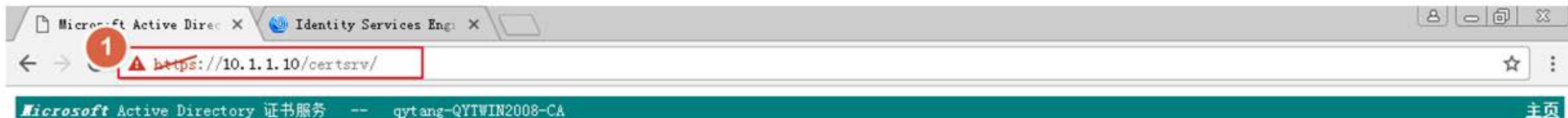
A success message dialog is displayed, indicating that the CSR was successfully generated. The dialog text is:

Successfully generated CSR(s) ✓
Certificate Signing request(s) generated:
QYTISE2-Master #Multi-Use
Click Export to download CSR(s) or OK to return to list of CSR(s) screen

The 'Export' button is highlighted with a red circle and the number 4. The 'Generate' button is highlighted with a red circle and the number 3.

ISE 申请证书 -1

- 申请证书



欢迎使用

使用此网站为您的 Web 浏览器、电子邮件客户端 或其他程序申请证书。通过使用证书，您可以向通过 Web 进行通信的用户确认您的身份、签名并加密 邮件，并根据您申请的证书类型执行其他 安全任务。

您也可以使用此网站下载证书颁发机构(CA)证书、证书链，或证书吊销列表(CRL)，或者查看挂起 申请的状态。

有关 Active Directory 证书服务的详细信息，请参阅 [Active Directory 证书服务文档](#)。

2 一个任务：

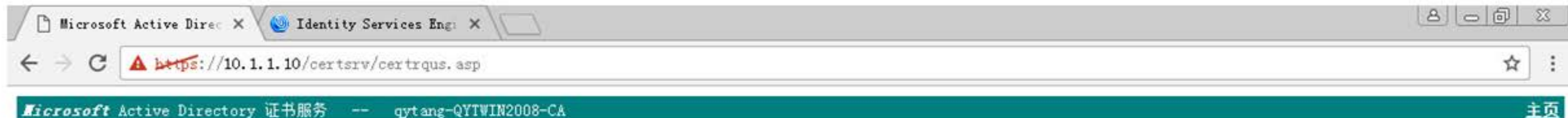
[申请证书](#)

[查看挂起的证书申请的状态](#)

[下载 CA 证书、证书链或 CRL](#)

ISE 申请证书 -2

- 选择高级证书申请



申请一个证书

选择一个证书类型:

[用户证书](#)

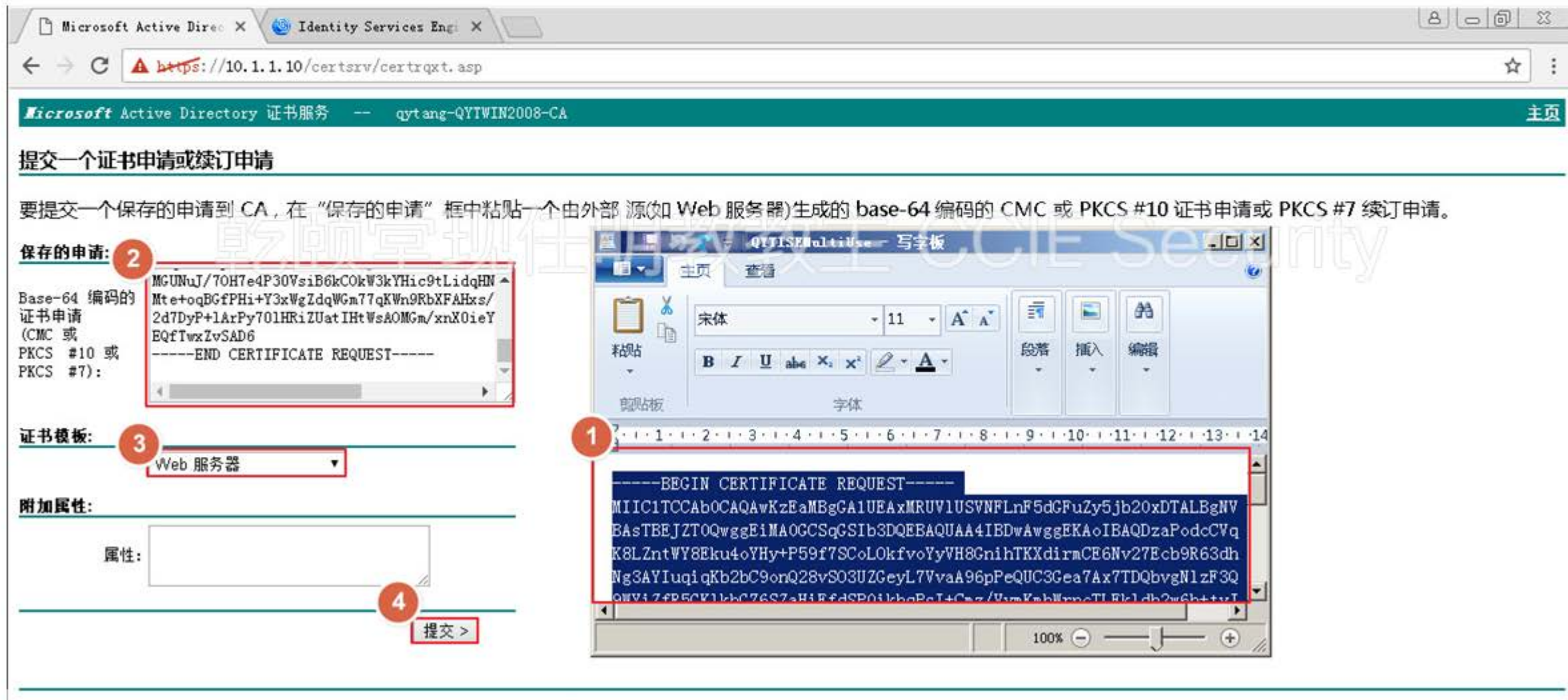
1

或者, 提交一个 [高级证书申请](#)。

乾颐堂现任明教教主 CCIE Security

ISE 申请证书 -3

- 打开 ISE 生成的 CSR 文件，粘贴到证书申请页面，提交申请



The screenshot shows the 'Identity Services Engine' web interface for submitting a certificate request. The page title is 'Microsoft Active Directory 证书服务' and the URL is 'https://10.1.1.10/certsrv/certrqxt.asp'. The main heading is '提交一个证书申请或续订申请'. Below this, there is a text box for '保存的申请:' containing a Base-64 encoded CSR. A red box labeled '2' highlights this text. To the right, a Notepad window shows the raw CSR text, with a red box labeled '1' highlighting the 'BEGIN CERTIFICATE REQUEST' line. Below the text box, there is a dropdown menu for '证书模板:' set to 'Web 服务器', with a red box labeled '3' around it. At the bottom, there is a '提交 >' button, with a red box labeled '4' around it.

要提交一个保存的申请到 CA，在“保存的申请”框中粘贴一个由外部源(如 Web 服务器)生成的 base-64 编码的 CMC 或 PKCS #10 证书申请或 PKCS #7 续订申请。

保存的申请: 2

```

MGUNuJ/7OH7e4P30VsiB6kC0kW3kYHic9tLidqHN
Mte+oqBGfPHi+Y3xWgZdqWgm77qKwn9RbXFAHxs/
2d7DyP+lArPy701HRiZUatIHtWsaOMGm/xnX0ieY
EQfTwxZvSAD6
-----END CERTIFICATE REQUEST-----
  
```

证书模板: 3

Web 服务器

附加属性:

属性:

4 提交 >

1

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC1TCCAAbOCAQAvKzEaMBGGA1UEAxMRUV1USVNFlnF5dGFuZy5jb20xDTALBgNV
BAstBEJZT0QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDzaPodcCVq
K8LZntWY8Eku4oYHY+P59f7SCoLokfvoYyVH8GnihTKXdirMCE6Nv27Ecb9R63dh
Ng3AYIuqiQKb2bC9onQ28vS03UZGeyL7VvaA96pPeQUC3Gea7Ax7TDQbvgN1zF3Q
QWV4ZfP5CV1bCZ6S7aHfEdSP01khpPcI4Cag/VmKahWpncTLFlLdh2wGhttuI
  
```


ISE 申请证书 -4

- 下载设备证书

Microsoft Active Directory 证书服务 -- qytang-QYTWIN2008-CA 主页

证书已颁发

您申请的证书已颁发给您。

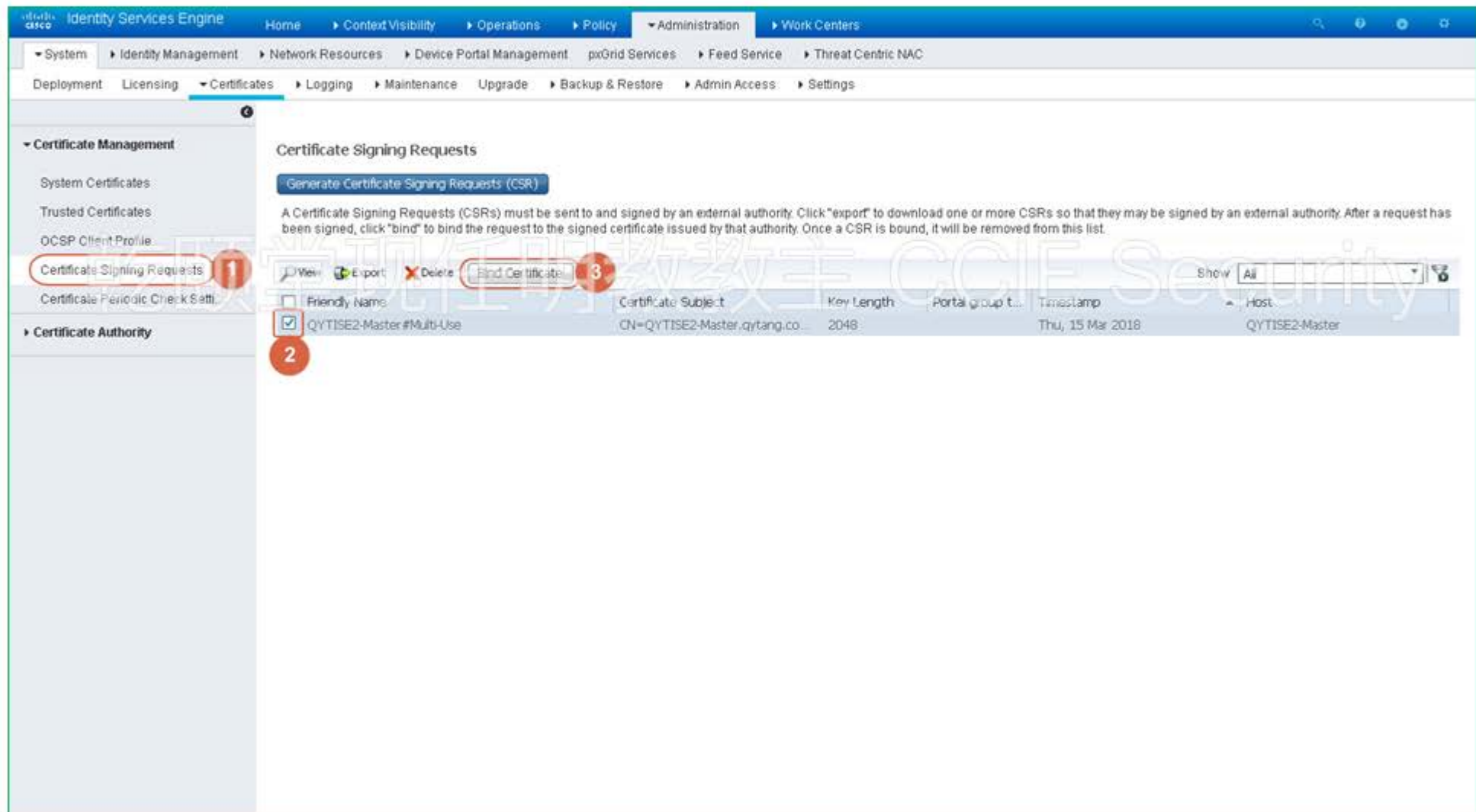
1 DER 编码 或 Base 64 编码

[下载证书](#)

[下载证书链](#)

ISE 绑定设备证书 - 1

- ISE 绑定设备证书



The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation menu at the top includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The left sidebar shows the Certificate Management section, with 'Certificate Signing Requests' highlighted. The main content area is titled 'Certificate Signing Requests' and contains a 'Generate Certificate Signing Requests (CSR)' button. Below this, there is a text block explaining that CSRs must be sent to and signed by an external authority. A table of CSRs is displayed, with columns for Certificate Subject, Key Length, Portal group t..., Timestamp, and Host. The first row is selected, and a checkbox is checked. A 'Bind Certificate' button is highlighted with a red circle and the number 3. A red circle with the number 2 is placed over the checkbox for 'QYTISE2-Master#Multi-Use'.

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal group t...	Timestamp	Host
<input checked="" type="checkbox"/>	QYTISE2-Master#Multi-Use	CN=QYTISE2-Master.qytang.co...	2048		Thu, 15 Mar 2018	QYTISE2-Master

ISE 绑定设备证书 - 2

- 安装设备证书需要导致设备服务重启，时间比较长

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Deployment > Licensing > Certificates > Logging > Maintenance > Upgrade > Backup & Restore > Admin Access > Settings

Certificate Management

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings

Certificate Authority

Bind CA Signed Certificate

* Certificate File 1

Friendly Name 2

Validate Certificate Extensions

Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- Portal: Use for portal

* Portal group tag 3

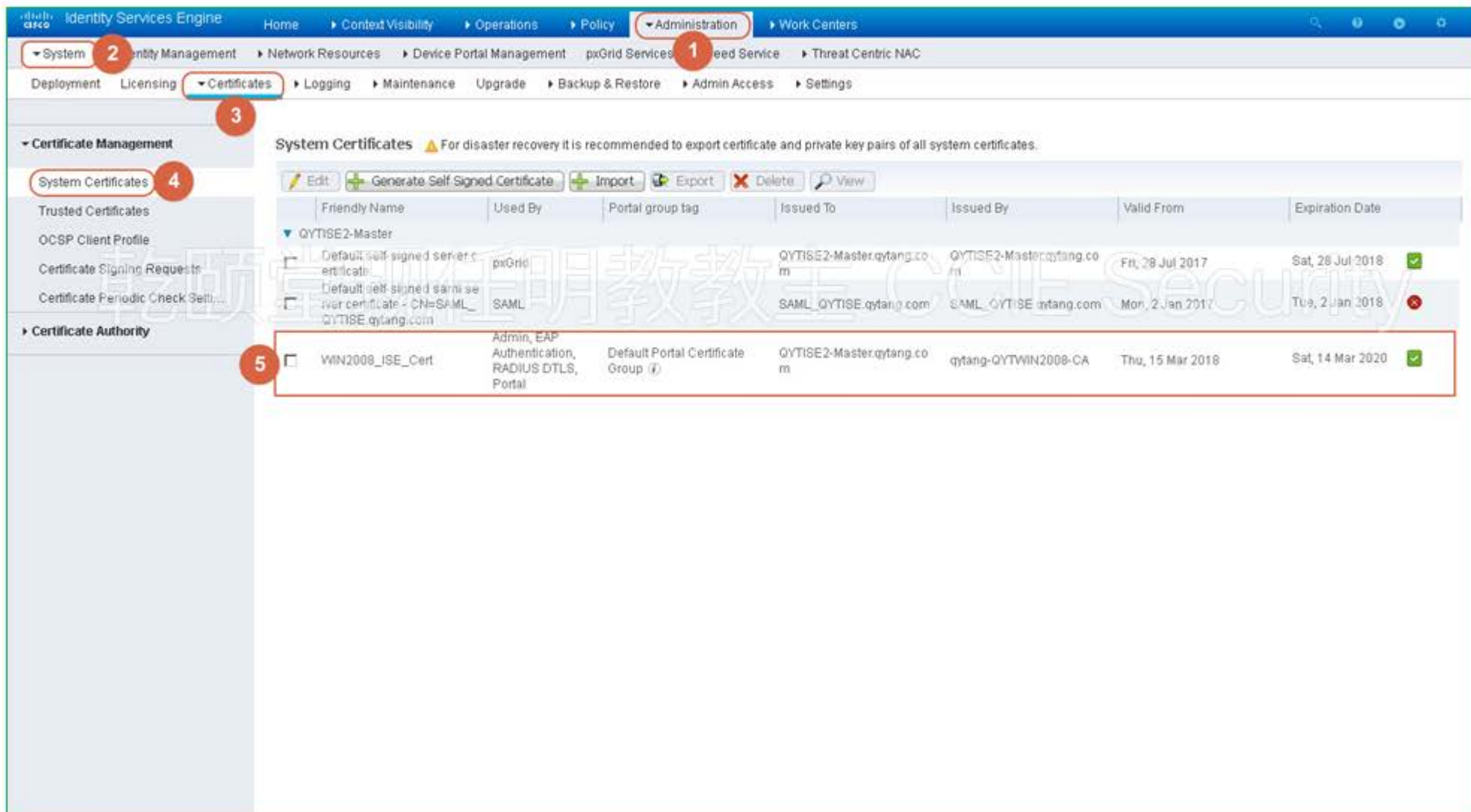
Portal(s) using this tag

BYOD Portal (default)	Blacklist Portal (default)
Certificate Provisioning Portal (default)	Client Provisioning Portal (default)
Hotspot Guest Portal (default)	MDM Portal (default)
My Devices Portal (default)	Self-Registered Guest Portal (default)
Sponsor Portal (default)	Sponsored Guest Portal (default)

4

查看 ISE 的设备证书

- 查看 ISE 的设备证书



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is: Administration > Certificates > System Certificates. The page displays a table of system certificates. A red box highlights the 'WIN2008_ISE_Cert' certificate, which is used for Admin, EAP Authentication, RADIUS DTLS, and Portal. The certificate was issued by 'qytang-QYTWIN2008-CA' on 'Thu, 15 Mar 2018' and expires on 'Sat, 14 Mar 2020'.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
QYTISE2-Master								
<input type="checkbox"/>	Default self-signed server certificate	pxGrid		QYTISE2-Master.qytang.com	QYTISE2-Master.qytang.com	Fri, 29 Jul 2017	Sat, 28 Jul 2018	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Default self-signed server certificate - CN=SAML-QYTISE.qytang.com	SAML		SAML_QYTISE.qytang.com	SAML_QYTISE.qytang.com	Mon, 2 Jan 2017	Tue, 2 Jan 2018	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	WIN2008_ISE_Cert	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group (7)	QYTISE2-Master.qytang.com	qytang-QYTWIN2008-CA	Thu, 15 Mar 2018	Sat, 14 Mar 2020	<input checked="" type="checkbox"/>



3.2 添加SCEP证书服务器

ISE 添加 SCEP 证书服务器 -1

- ISE 添加 SCEP 证书服务器。完成 SCEP CA 添加后，ISE 会获取 ISE 的身份证书，以及 CA 服务器根证书和 SCEP 服务的 RA 证书。

Microsoft Active Direc X Identity Services Engi X

https://10.1.1.12/admin/#administration/administration_system/administration_system_certificates/certificates_cert_auth/certificates_cert_auth_external_ca_s

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

Certificate Authority

Certificate Authority Certificates

Internal CA Settings

1 Certificate Templates

External CA Settings

External CA Settings

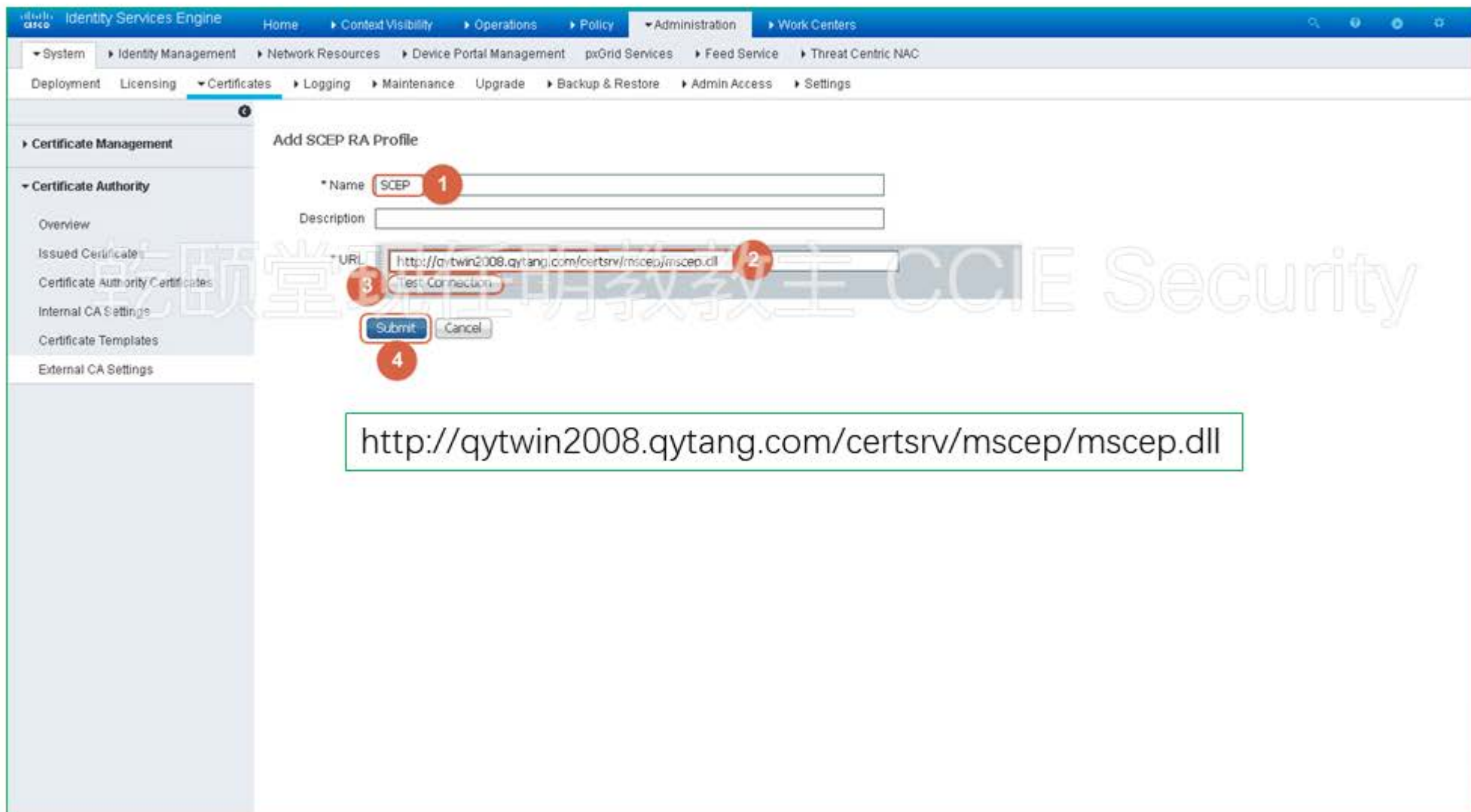
SCEP CA Profiles (SCEP-Simple Certificate Enrollment Protocol)

2 Edit Add Delete

<input type="checkbox"/>	Name	Description	URL	CA Cert Name
No data available				

ISE 添加 SCEP 证书服务器 -2

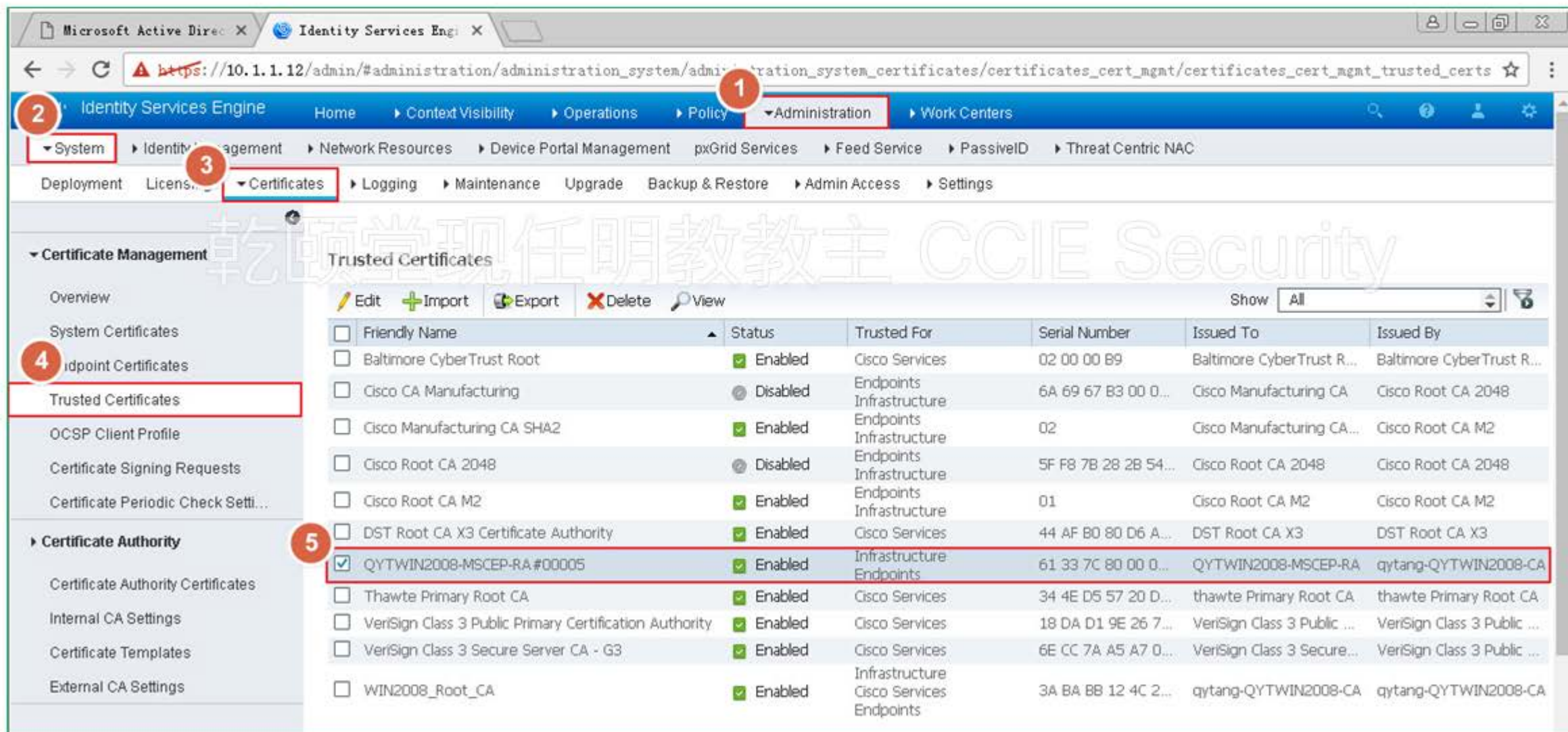
- 填写证书服务器信息，可以使用 Test Connection 测试连通性



http://qytwin2008.qytang.com/certsrv/mscep/mscep.dll

查看 SCEP 生成的 RA 证书

- 添加成功



乾颐堂现任明教教主 CCIE Security

<input type="checkbox"/>	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By
<input type="checkbox"/>	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust R...	Baltimore CyberTrust R...
<input type="checkbox"/>	Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 0...	Cisco Manufacturing CA	Cisco Root CA 2048
<input type="checkbox"/>	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA...	Cisco Root CA M2
<input type="checkbox"/>	Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54...	Cisco Root CA 2048	Cisco Root CA 2048
<input type="checkbox"/>	Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2
<input type="checkbox"/>	DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A...	DST Root CA X3	DST Root CA X3
<input checked="" type="checkbox"/>	QYWIN2008-MSCEP-RA#00005	Enabled	Infrastructure Endpoints	61 33 7C 80 00 0...	QYWIN2008-MSCEP-RA	qytang-QYWIN2008-CA
<input type="checkbox"/>	Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D...	thawte Primary Root CA	thawte Primary Root CA
<input type="checkbox"/>	VeriSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7...	VeriSign Class 3 Public ...	VeriSign Class 3 Public ...
<input type="checkbox"/>	VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 0...	VeriSign Class 3 Secure...	VeriSign Class 3 Public ...
<input type="checkbox"/>	WIN2008_Root_CA	Enabled	Infrastructure Cisco Services Endpoints	3A BA BB 12 4C 2...	qytang-QYWIN2008-CA	qytang-QYWIN2008-CA



3.3 创建BYOD证书申请模板

创建证书申请模版 - 1

- ISE 创建证书申请模板

乾師堂现任明教教主 CCIE Security

<input type="checkbox"/>	Template Name	Description	Key Type	Key Size	Curve Type
<input type="checkbox"/>	CA_SERVICE_Certificat...	This template will be u...	RSA	2048	N/A
<input type="checkbox"/>	EAP_Authentication_C...	This template will be u...	RSA	2048	N/A
<input type="checkbox"/>	pxGrid_Certificate_Te...	This template will be u...	RSA	2048	N/A

创建证书申请模版 - 2

- 填写模板相关信息

The screenshot displays the 'Add Certificate Template' configuration page in the Cisco Identity Services Engine (ISE) web interface. The page is titled 'Add Certificate Template' and contains several input fields and options for configuring a new certificate template. The fields are as follows:

- * Name:** BYOD_SCEP (Step 2)
- Description:** This is for BYOD (Step 3)
- Subject:**
 - Common Name (CN): \$UserName\$ (n)
 - Organizational Unit (OU): BYOD
 - Organization (O):
 - City (L): beijing (Step 4)
 - State (ST): beijing
 - Country (C): CN
- Subject Alternative Name (SAN):** MAC Address
- Key Type:** RSA
- Key Size:** 2048
- * SCEP RA Profile:** SCEP (Step 5)
- Extended Key Usage:** Client Authentication Server Authentication

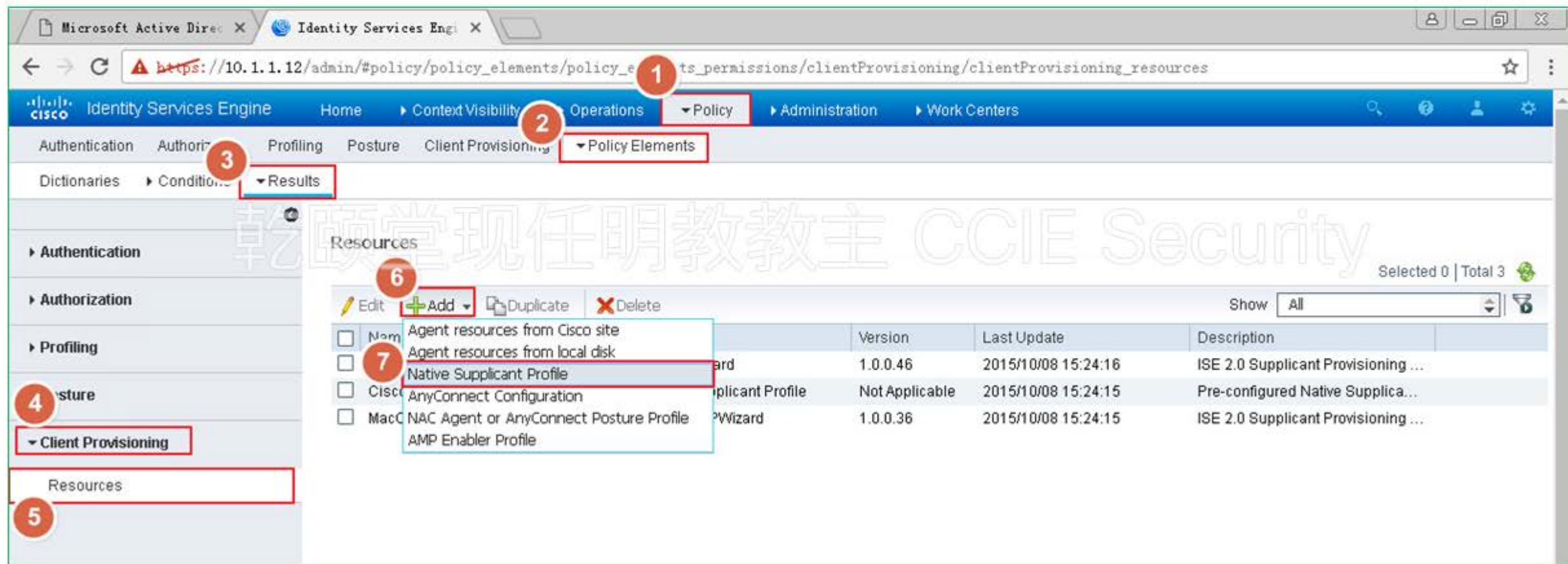
At the bottom of the page, there is a **Submit** button (Step 6) and a **Cancel** button.



3.4 Native Supplicant Profile

创建 Native Supplicant Profile - 1

- 创建本地请求配置文件



乾颐堂现任明教教主 CCIE Security

Resources Selected 0 | Total 3

Name	Version	Last Update	Description
Agent resources from Cisco site			
Agent resources from local disk			
Native Supplicant Profile			
Cisco AnyConnect Configuration	1.0.0.46	2015/10/08 15:24:16	ISE 2.0 Supplicant Provisioning ...
MacC NAC Agent or AnyConnect Posture Profile	Not Applicable	2015/10/08 15:24:15	Pre-configured Native Supplica...
AMP Enabler Profile	1.0.0.36	2015/10/08 15:24:15	ISE 2.0 Supplicant Provisioning ...

创建 Native Supplicant Profile - 2

- 编辑本地请求配置文件

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Native Supplicant Profile > New Profile

Native Supplicant Profile

Name BYOD_Profile

Description

Operating System ALL

Wireless Profile(s)
Multiple SSIDs can be configured, and the first profile will be the active profile. For Windows or Mac, the Proxy settings of the first profile will be applied globally (i.e. to all subsequent profiles).
Proxy Auto-Config File URL will be used for automatic configuration of proxy settings. Supported by iOS, MAC OS, Windows & Android 5.0 or above.
If no Proxy Auto-Config File URL is defined then the Proxy host/port will be used for all operating systems, otherwise it will just be used for early (pre 5.x) versions of Android.

Selected 0 | Total 0

Edit Add Duplicate Delete

SSID Name	Proxy Auto-Config File ...	Proxy Host/IP	Port	Security	Allowed Protocol	Certificate Template
No data available						

创建 Native Supplicant Profile - 3

- 编辑本地请求配置文件

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The main window displays the 'Wireless Profile' configuration dialog. The dialog is titled 'Wireless Profile' and contains several fields and sections. Red circles with numbers 1, 2, 3, and 4 highlight specific configuration points:

- 1. SSID Name: BYOD
- 2. Allowed Protocol: TLS
- 3. Authentication Mode: User
- 4. Save button

The background shows the ISE web interface with the following navigation path: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Client Provisioning > Policy Elements > Results. The 'Wireless Profile(s)' section is active, showing a table with columns for SSID Name, Allowed Protocol, and Certificate Template. The 'Optional Settings' section is expanded, showing 'Windows Setting' and 'iOS Settings'.

创建 Native Supplicant Profile - 4

- 提交

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The browser address bar displays the URL: `https://10.1.1.12/admin/#policy/policy_elements/policy_elements_permissions/clientProvisioning/clientProvisioning_resources`. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The main content area is titled "Policy Elements" and shows a table of resources. A red circle with the number "1" highlights the "Submit" button at the bottom of the configuration form.

Multiple SSIDs can be configured, and the first profile will be the active profile. For windows or mac, the Proxy settings of the first profile will be applied globally (i.e. to all subsequent profiles).
Proxy Auto-Config File URL will be used for automatic configuration of proxy settings. Supported by iOS, MAC OS, Windows & Android 5.0 or above.
If no Proxy Auto-Config File URL is defined then the Proxy host/port will be used for all operating systems, otherwise it will just be used for early (pre 5.x) versions of Android.

SSID Name	Proxy Auto-Config File ...	Proxy Host/IP	Port	Security	Allowed Protocol	Certificate Template
<input type="checkbox"/> BYOD				WPA2 Enterprise	TLS	BYOD_SCEP

Wired Profile

Allowed Protocol * PEAP

Certificate Template Not Required

Optional Settings

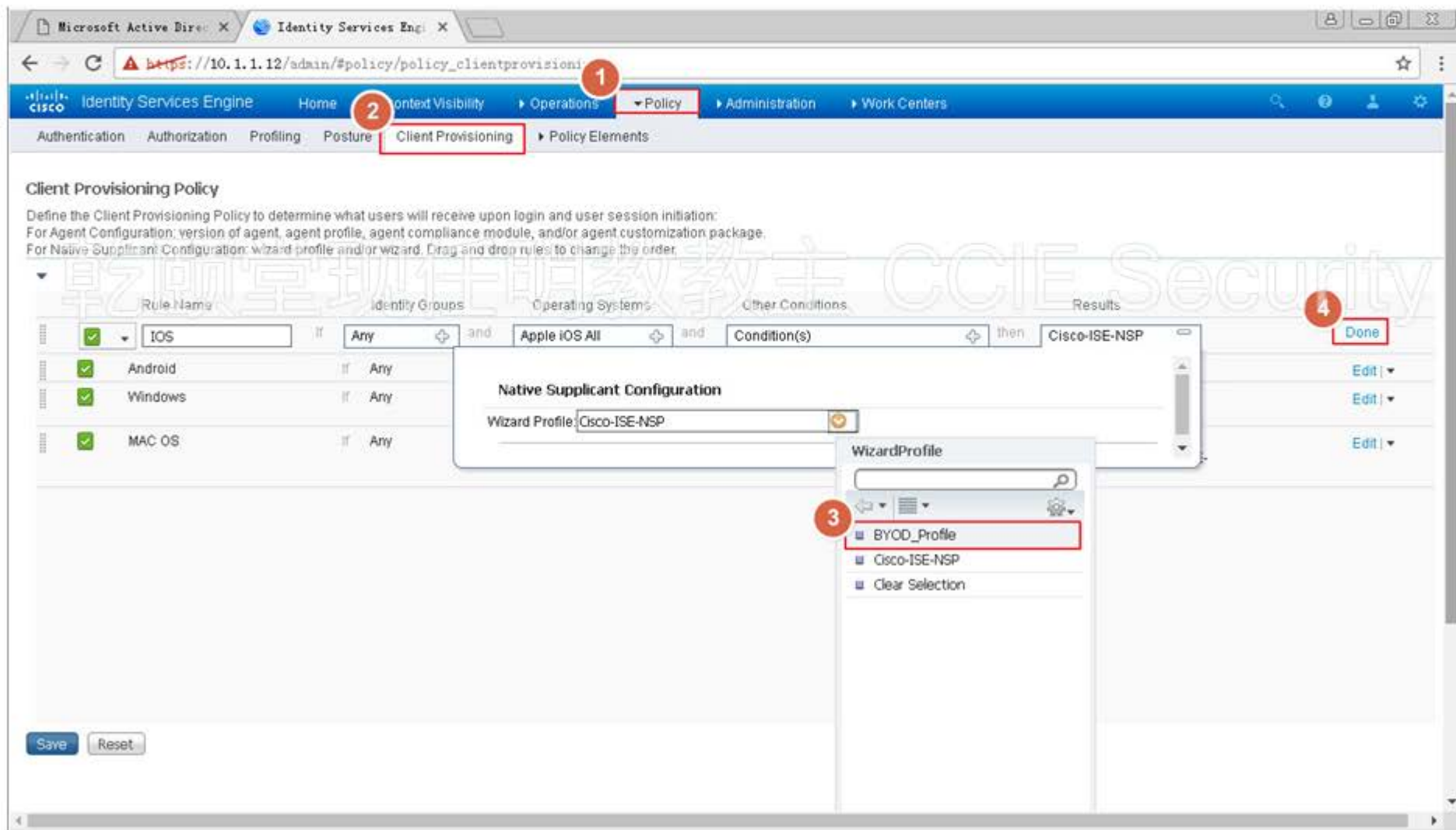
1 Submit Cancel



3.5 Client Provisioning策略

修改 Client Provisioning 策略 - 1

- 修改 Client Provisioning 策略



The screenshot shows the Cisco Identity Services Engine (ISE) web interface for configuring a Client Provisioning Policy. The browser address bar shows the URL: `https://10.1.1.12/admin/#policy/policy_clientprovisioning`. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The main menu has Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. The Client Provisioning Policy configuration page is displayed, with the following details:

- Client Provisioning Policy**: Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation. For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package. For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.
- Rule Configuration**:

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	Any	Apple iOS All	Condition(s)	Cisco-ISE-NSP
Android	Any			
Windows	Any			
MAC OS	Any			
- Native Supplicant Configuration**: Wizard Profile: Cisco-ISE-NSP
- WizardProfile** dropdown menu: BYOD_Profile, Cisco-ISE-NSP, Clear Selection
- Buttons**: Save, Reset, Done, Edit

修改 Client Provisioning 策略 - 2

- 修改 Client Provisioning 策略

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any	and Apple iOS All	and Condition(s)	then BYOD_Profile 1
Android	If Any	and Android	and Condition(s)	then BYOD_Profile 2
Windows	If Any	and Windows All	and Condition(s)	then WinSPWiz:1.1.0.0.46 And BYOD_Profile 3
MAC OS	If Any	and Mac OSX	and Condition(s)	then MacOsXSPWizard 1.0.0.36 And Cisco-ISE- NSP

Save Reset



3.6 ISE集成MS域

添加 AD 域集成 - 1

- ISE 加域

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The browser address bar displays the URL: `https://10.1.1.12/admin/#administration/administration_identitymanagement/administration_identitymanagement_external`. The navigation menu is expanded to show the following path: **Administration** > **External Identity Sources**. The left-hand navigation pane shows the following structure:

- External Identity Sources
 - Certificate Authentication Profile
 - Active Directory
 - LDAP
 - ODBC
 - RADIUS Token
 - RSA SecurID
 - SAML Id Providers

The main content area shows the configuration page for an Active Directory source. The **Add** button is highlighted. The configuration details include:

- Join Point Name:
- Active Directory Domain:

The status at the bottom of the page is "No data available".

添加 AD 域集成 - 2

- 填写域名

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The browser address bar displays the URL: `https://10.1.1.12/admin/#administration/administration_identitymanagement/administration_identitymanagement_external`. The navigation menu includes: Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Administration, the path is: External Identity Sources > Active Directory.

The main content area shows the configuration for an Active Directory connection. The fields are:

- Join Point Name: Win2008-AD
- Active Directory Domain: qytang.com

Red boxes and numbers highlight the configuration steps:

- 1: Points to the Active Directory Domain field.
- 2: Points to the Submit button.

A watermark "乾堂现任明教教主 CCIE Security" is visible across the center of the screenshot.

添加 AD 域集成 - 3

- 用管理员账号加域

乾颐堂现任明教教主 CCIE Security

Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name administrator

* Password *****

Specify Organizational Unit

OK Cancel

ISE Node	ISE Node Role	Status	Domain Controller	Site
<input type="checkbox"/> QYTISE.qytang.com	STANDALONE	Not Joined		

添加 AD 域集成 - 4

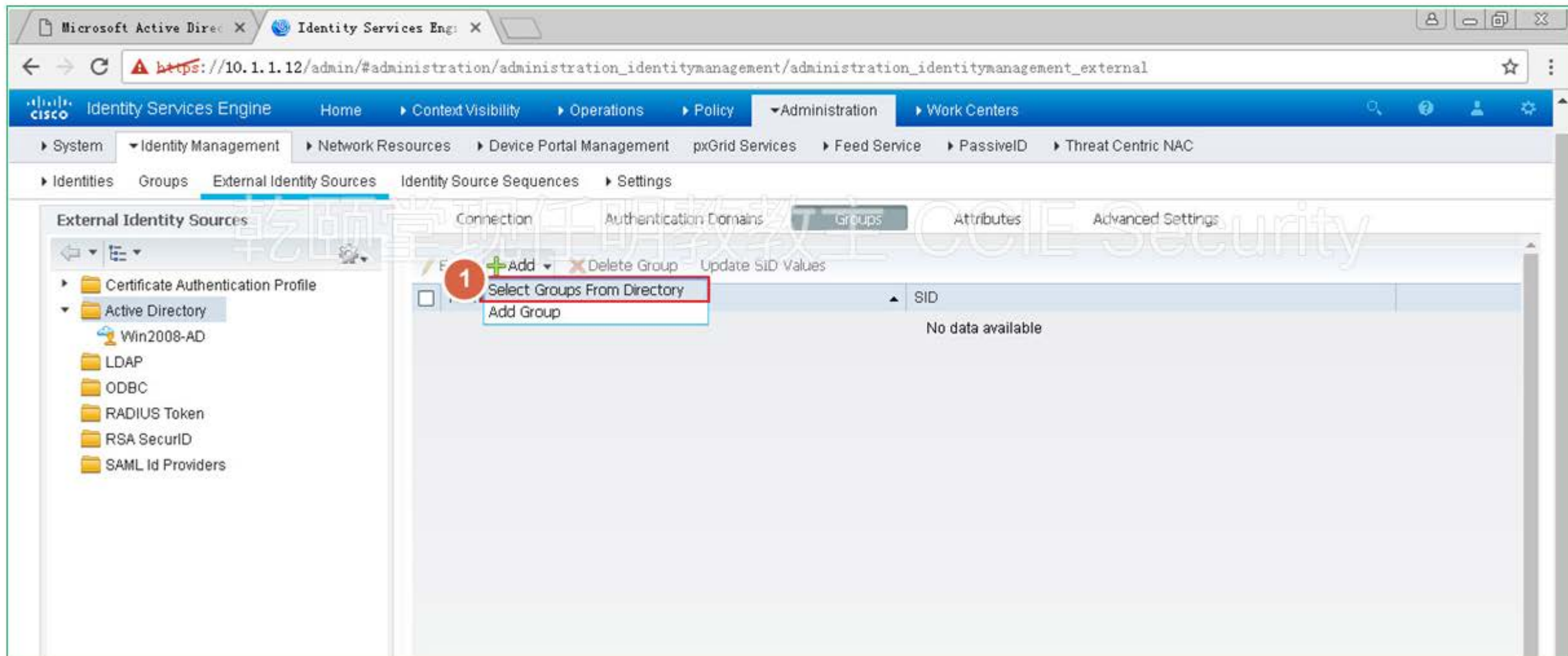
- 加域成功

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The browser address bar displays `https://10.1.1.12/admin/#administration/administration_identitymanagement/administration_identitymanagement_external`. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The left sidebar shows the 'External Identity Sources' section, with 'Active Directory' expanded to show 'Win2008-AD'. A modal dialog titled 'Join Operation Status' is open, displaying the following information:

Join Operation Status	
Status Summary: Successful	
ISE Node	Node Status
QYTISE.qytang.com	Completed.

提取 AD 域的组信息 - 1

- 提取组信息



The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The browser address bar shows the URL: `https://10.1.1.12/admin/#administration/administration_identitymanagement/administration_identitymanagement_external`. The navigation menu includes: Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The main navigation bar lists: System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, PassivID, and Threat Centric NAC. The sub-navigation bar includes: Identities, Groups, External Identity Sources, Identity Source Sequences, and Settings. The 'External Identity Sources' section is active, with tabs for Connection, Authentication Domains, Groups, Attributes, and Advanced Settings. The 'Groups' tab is selected, showing a table with a 'SID' column. A red circle with the number '1' highlights the 'Add' button, which has a dropdown menu open. The dropdown menu contains the options 'Select Groups From Directory' and 'Add Group'. The table currently displays 'No data available'.

提取 AD 域的组信息 - 2

- 提取 byod_group, employee_group 组信息

Select Directory Groups
This dialog is used to select groups from the Directory.

Domain: qytang.com
Name Filter: * SID Filter: * Type Filter: ALL

1 Retrieve Groups... 138 Groups Retrieved.

Name	Group SID	Group Type
<input checked="" type="checkbox"/> qytang.com/BYOD/employee_group 2	S-1-5-21-1256851807-319077736-1261551576-1103	GLOBAL
<input type="checkbox"/> qytang.com/Builtin/Account Operators	qytang.com/S-1-5-32-548	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Administrators	qytang.com/S-1-5-32-544	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Backup Operators	qytang.com/S-1-5-32-551	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Certificate Service DCOM Access	qytang.com/S-1-5-32-574	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Cryptographic Operators	qytang.com/S-1-5-32-569	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Distributed COM Users	qytang.com/S-1-5-32-562	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Event Log Readers	qytang.com/S-1-5-32-573	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Guests	qytang.com/S-1-5-32-546	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/IS_USRS	qytang.com/S-1-5-32-568	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Incoming Forest Trust Builders	qytang.com/S-1-5-32-557	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Network Configuration Operators	qytang.com/S-1-5-32-556	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Performance Log Users	qytang.com/S-1-5-32-559	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Performance Monitor Users	qytang.com/S-1-5-32-558	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Pre-Windows 2000 Compatible Ac...	qytang.com/S-1-5-32-554	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Print Operators	qytang.com/S-1-5-32-550	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Remote Desktop Users	qytang.com/S-1-5-32-555	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Replicator	qytang.com/S-1-5-32-552	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Server Operators	qytang.com/S-1-5-32-549	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Terminal Server License Servers	qytang.com/S-1-5-32-561	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Users	qytang.com/S-1-5-32-545	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Builtin/Windows Authorization Access Group	qytang.com/S-1-5-32-580	BUILTIN, DOMAIN LOCAL
<input type="checkbox"/> qytang.com/Users/Allowed RODC Password Replicat...	S-1-5-21-1256851807-319077736-1261551576-571	DOMAIN LOCAL

3 OK Cancel

提取 AD 域的组信息 - 3

- 提取成功

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation pane on the left is expanded to 'External Identity Sources' > 'Active Directory' > 'Win2008-AD'. The main content area is in the 'Groups' tab, displaying a table of extracted AD groups. A red circle '1' highlights the group name 'qytang.com\BYOD\employee_group'. At the bottom of the console, a red circle '2' highlights the 'Save' button.

Name	SID
qytang.com\BYOD\employee_group	S-1-5-21-1256851807-3190777736-1261551576-1103



4. WLC与ISE授权

4.1 创建NDG和Network Device

4.2 配置WLC ACL

4.3 配置ISE授权

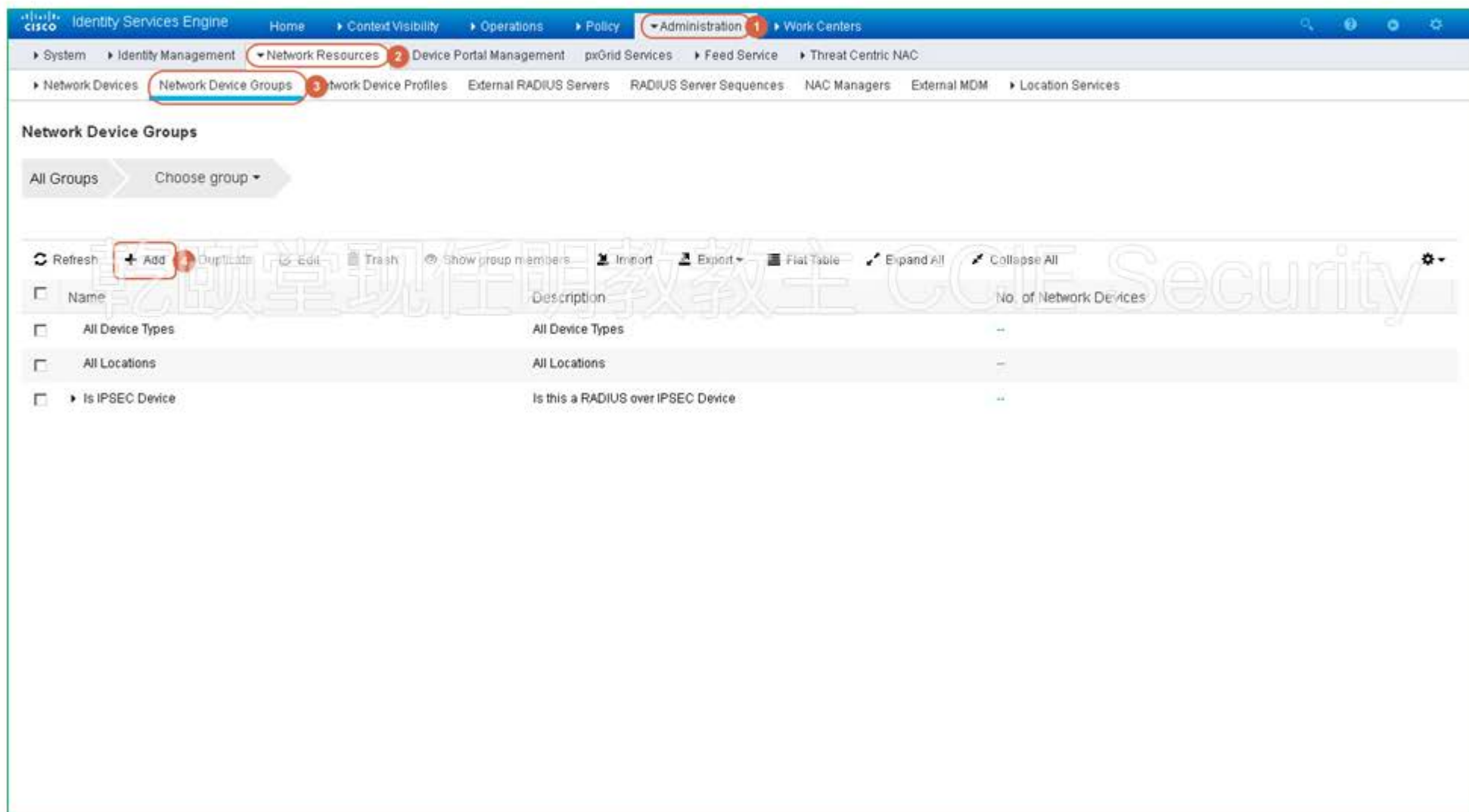
4.4 配置WLAN



4.1 创建NDG和Network Device

ISE 创建 NDG - 1

- 添加网络设备组



Network Device Groups

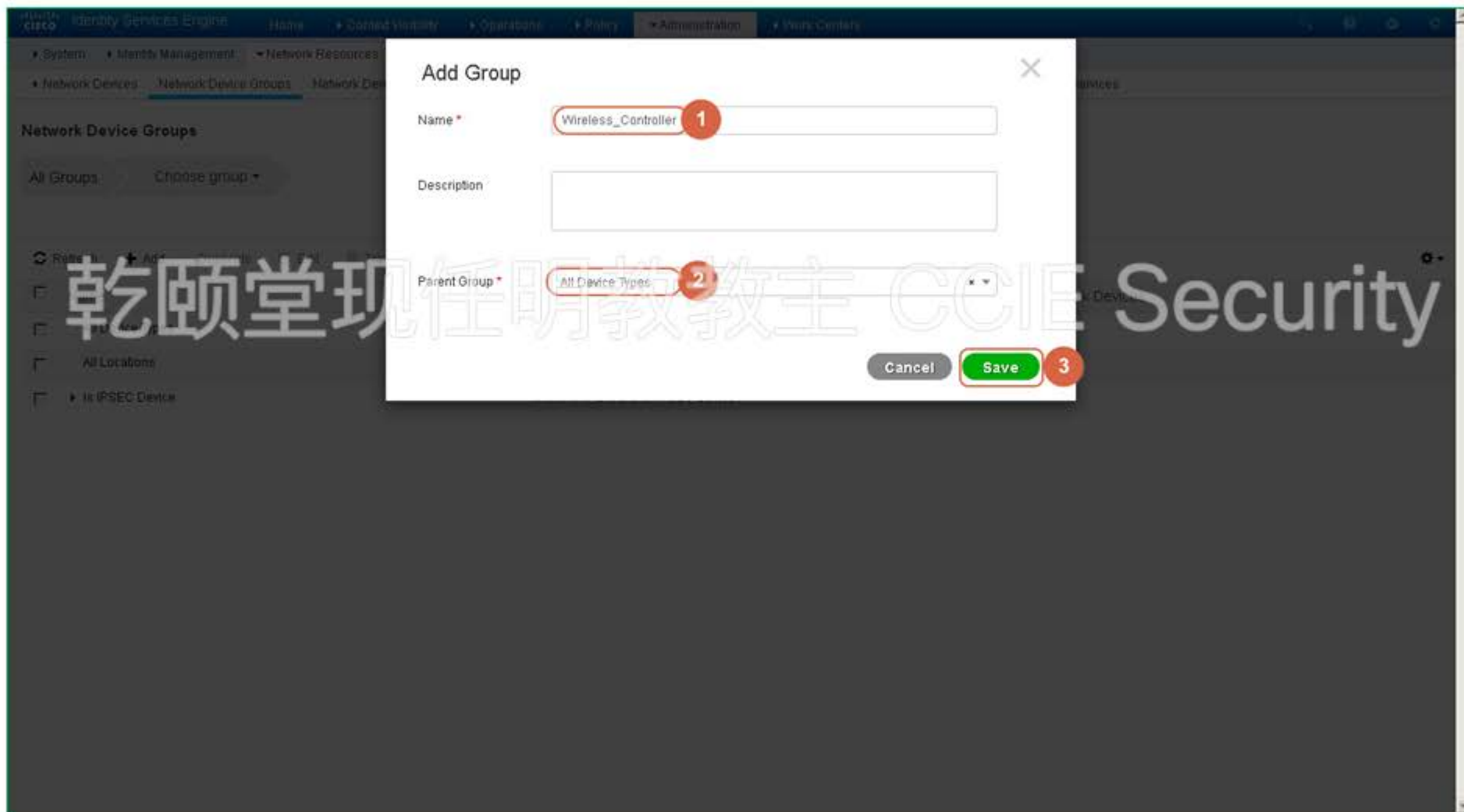
All Groups > Choose group ▾

Refresh + Add Duplicate Edit Trash Show group members Import Export Flat Table Expand All Collapse All

<input type="checkbox"/>	Name	Description	No. of Network Devices
<input type="checkbox"/>	All Device Types	All Device Types	--
<input type="checkbox"/>	All Locations	All Locations	--
<input type="checkbox"/>	Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

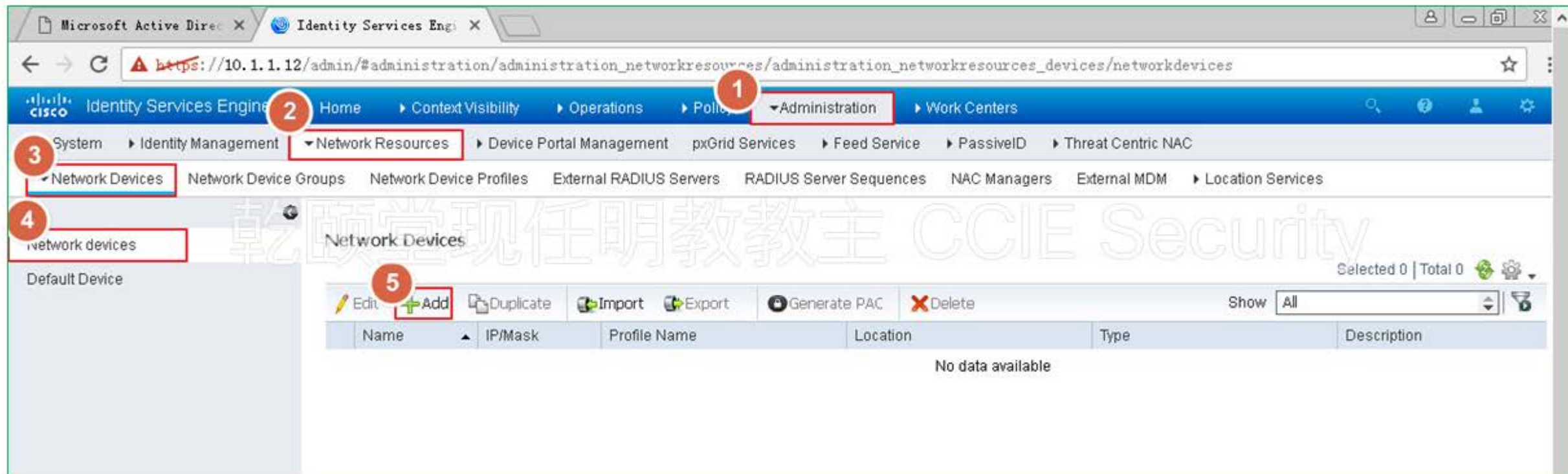
ISE 创建 NDG - 2

- 为网络设备组命名



ISE 添加 Device - 1

- 添加网络设备



Identity Services Engine Administration Console Screenshot:

- 1. Administration
- 2. Network Resources
- 3. Network Devices
- 4. Network Devices (Left Sidebar)
- 5. Add (Toolbar)

Network Devices Table:

Name	IP/Mask	Profile Name	Location	Type	Description
No data available					

ISE 添加 Device - 2

- 添加无线控制器

Network devices

Default Device

Network Devices List > New Network Device

Network Devices

* Name 5508-1

Description

* IP Address 10.1.1.100 / 32

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Device Type Wireless_Controller

Location All Locations

ISE 添加 Device - 3

- 填写预共享密钥

RADIUS Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

CoA Port

▶ TACACS Authentication Settings

▶ SNMP Settings

▶ Advanced TrustSec Settings



4.2 配置WLC ACL

WLC 上创建 ACL - 1

- 开启计数器

Microsoft Active Direc X Identity Services Eng X WLC-5508-1 X

← → ↻ <https://10.1.1.100/screens/frameset.html> ☆

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Save Configuration Ping Logout Refresh

Security

- ▶ AAA
- ▶ Local EAP
 - Advanced EAP
- ▶ Priority Order
- ▶ Certificate
- 2 Access Control Lists
 - Access Control Lists
 - CPU Access Control Lists
 - FlexConnect ACLs
 - Layer2 ACLs
- ▶ Wireless Protection Policies
- ▶ Web Auth
 - TrustSec SXP
 - Local Policies
- ▶ Advanced

Access Control Lists

Enable Counters 3

Name	Type
------	------

Foot Notes

1. Counter configuration is global for acl and layer2acl.

5 New... 4 Apply

乾颐堂现任明教教主 CCIE Security

WLC 上创建 ACL - 2

- 创建 ACL “portal”

The screenshot shows the Cisco WLC Security configuration page for an Access Control List named 'portal'. The 'General' tab is active, showing the Access List Name as 'portal' and Deny Counters as 0. A table below lists the ACL rules with their sequence numbers, actions, source and destination IP/masks, protocols, ports, and the number of hits.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 /	0.0.0.0 /	UDP	Any	DNS	Any	Any	89
2	Permit	0.0.0.0 /	0.0.0.0 /	UDP	DNS	Any	Any	Any	89
3	Permit	10.1.1.141 / 255.255.255.255	0.0.0.0 /	Any	Any	Any	Any	Any	91
4	Permit	0.0.0.0 /	10.1.1.141 /	Any	Any	Any	Any	Any	102
5	Permit	0.0.0.0 /	172.217.0.0 /	Any	Any	Any	Any	Any	1437
6	Permit	172.217.0.0 /	0.0.0.0 /	Any	Any	Any	Any	Any	1855
7	Permit	0.0.0.0 /	216.58.0.0 /	Any	Any	Any	Any	Any	2
8	Permit	216.58.0.0 /	0.0.0.0 /	Any	Any	Any	Any	Any	3
9	Deny	0.0.0.0 /	0.0.0.0 /	Any	Any	Any	Any	Any	1208

获取放行地址的技巧

The screenshot shows a Wireshark capture of a DNS query and response. The filter is set to 'dns and ip.addr == 30.1.1.2'. The packet list shows a query from 30.1.1.2 to 10.1.1.10 for 'android.clients.google.com'. The packet details show the query type as 'Standard query' and the response as 'Standard query response'. The response contains several records, including a CNAME record for 'android.clients.google.com' pointing to 'lh5.googleusercontent.com'.

In the foreground, a terminal window shows the command 'nslookup android.clients.google.com' and its output:

```

管理员: C:\Windows\system32\cmd.exe - nslookup
Address: ::1
非权威应答:
名称:   play.l.google.com
Addresses: 2607:f8b0:4007:807::200e
          172.217.11.174
Aliases: play.google.com
> android.clients.google.com
服务器:   unknown
Address:  ::1
非权威应答:
名称:   android.l.google.com
Addresses: 216.58.219.46
          216.58.217.206
          172.217.5.206
          172.217.4.142
          172.217.11.174
          172.217.14.110
          172.217.11.78
          172.217.14.78
          216.58.216.14
          216.58.216.46
  
```

The terminal output shows that the domain 'android.clients.google.com' is resolved to multiple IP addresses, including 216.58.219.46, 216.58.217.206, 172.217.5.206, 172.217.4.142, 172.217.11.174, 172.217.14.110, 172.217.11.78, 172.217.14.78, 216.58.216.14, and 216.58.216.46.

The Wireshark packet details for the response (Frame 724) show the following records:

- Standard query response 0x4603 A android.clients.google.com CNAME andro...
- Standard query response 0xdec5 A android.clients.google.com CNAME andro...
- Standard query 0xf9cd A aeventlog.beacon.qq.com
- Standard query 0x317f A aeventlog.beacon.qq.com OPT
- Standard query 0x317f A aeventlog.beacon.qq.com OPT
- Standard query response 0x317f A aeventlog.beacon.qq.com A 101.227.130...
- Standard query response 0xf9cd A aeventlog.beacon.qq.com A 101.227.130...
- Standard query 0x983e A lh5.googleusercontent.com
- Standard query response 0x983e A lh5.googleusercontent.com CNAME google...
- Standard query 0xd5db A connectivitycheck.smartisan.com
- Standard query 0x1027 A connectivitycheck.smartisan.com OPT
- Standard query 0x1027 A connectivitycheck.smartisan.com OPT
- Standard query response 0x1027 A connectivitycheck.smartisan.com CNAME ...
- Standard query response 0xd8db A connectivitycheck.smartisan.com CNAME ...
- Standard query 0xf9f0 A connectivitycheck.smartisan.com
- Standard query response 0xf9f0 A connectivitycheck.smartisan.com CNAME ...
- Standard query 0xf310 A connectivitycheck.smartisan.com
- Standard query 0x8f37 A connectivitycheck.smartisan.com OPT
- Standard query 0x8f37 A connectivitycheck.smartisan.com OPT
- Standard query response 0x8f37 A connectivitycheck.smartisan.com CNAME ...
- Standard query response 0xf310 A connectivitycheck.smartisan.com CNAME ...
- Standard query 0x8765 A connectivitycheck.smartisan.com
- Standard query 0x74af A connectivitycheck.smartisan.com OPT
- Standard query 0x74af A connectivitycheck.smartisan.com OPT
- Standard query response 0x877e A connectivitycheck.smartisan.com OPT

The packet bytes pane shows the raw DNS data in hexadecimal and ASCII:

```

0000  00 50 56 ab 86 de 00 19 56 84 2a c1 08 00 45 00  .PV.... V.*...E.
0010  00 47 27 0d 40 00 3f 11 ea 8b 1e 01 01 02 0a 01  .G'.@.?. .....
0020  01 0a c9 6f 00 35 00 33 0c 5b 98 3e 01 00 00 01  ...o.5.3 .[>...
0030  00 00 00 00 00 00 03 6c 68 35 11 67 6f 6f 67 6c  .....l h5.googl
  
```

WLC 上创建 ACL - 3

- 创建 ACL “internet_only”

The screenshot shows the Cisco WLC configuration page for Access Control Lists. The 'Access List Name' is set to 'internet_only'. The 'Deny Counters' are set to 0. The table below shows the configured rules:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Deny	0.0.0.0	10.1.1.100	Any	Any	Any	Any	Any	0
2	Permit	0.0.0.0	0.0.0.0	Any	Any	Any	Any	Any	27324

WLC 上创建 ACL - 4

- 创建 ACL “permit_all”

The screenshot shows the Cisco WLC configuration page for 'Access Control Lists > Edit'. The 'General' tab is selected, and the 'Access List Name' is set to 'permit_all'. The 'Deny Counters' are 0. A table below shows the ACL rules:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
<u>1</u>	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

The first rule is highlighted with a red box. The interface also includes a left sidebar with navigation options like AAA, Local EAP, and Access Control Lists, and a top navigation bar with options like MONITOR, WLANs, and SECURITY.



4.3 配置ISE授权

修改授权 Profile - 1

- 修改授权 Profile

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the configuration tree with the following items highlighted: Policy Elements (1), Rest (2), Authorizations (3), and Authorization Profiles (4). The main content area displays the 'Standard Authorization Profiles' page, which includes a table of profiles and a list of profiles.

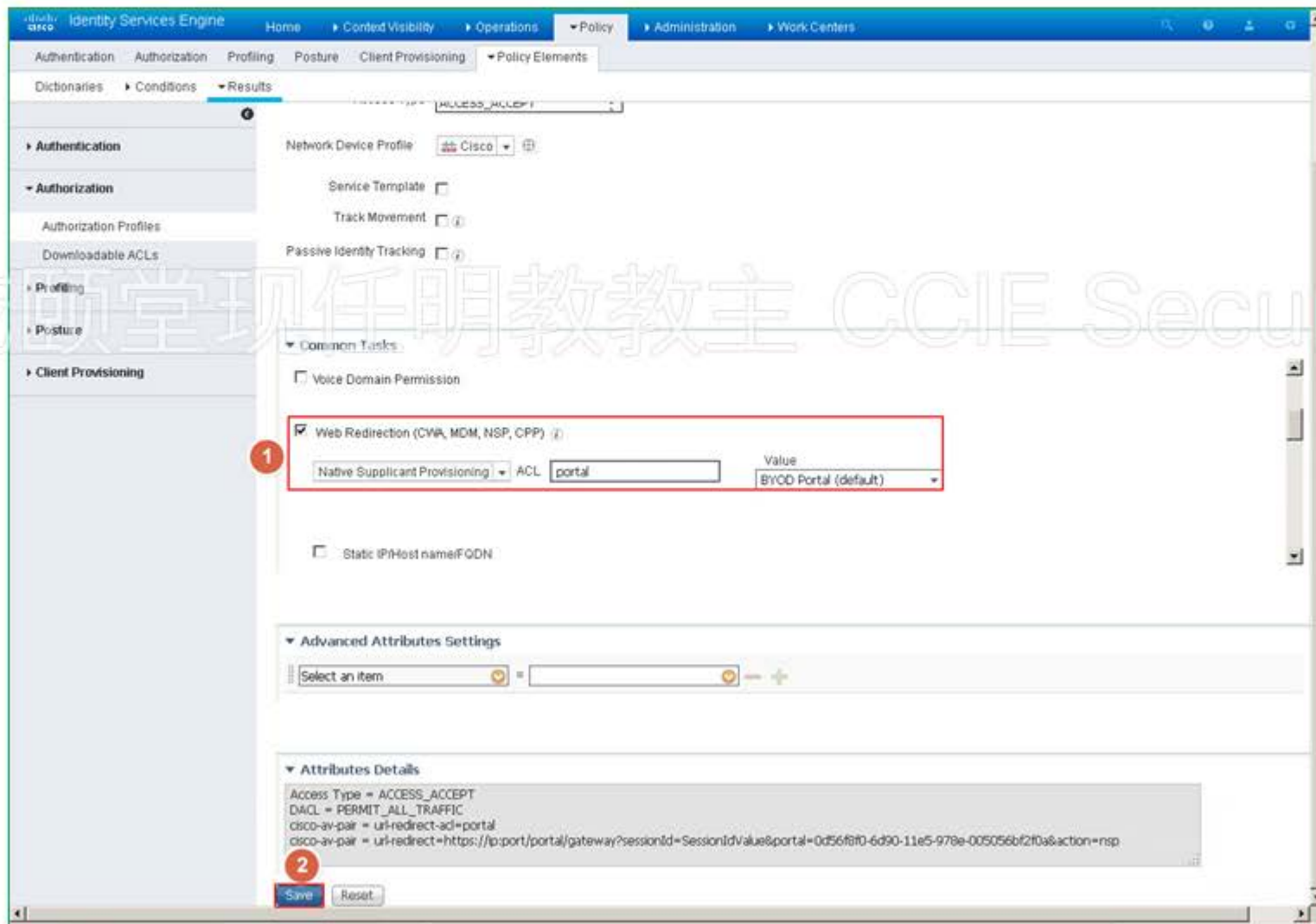
Standard Authorization Profiles
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Selected 0 | Total 7

Name	Profile	Description
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you cont
Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
Cisco_bAuth	Cisco	Default Profile used to redirect users to the CWA portal.
NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
DenyAccess		Default Profile with access type as Access-Reject
PermitAccess		Default Profile with access type as Access-Accept

修改授权 Profile - 2

- 重定向到 “portal”



Identity Services Engine

Home > Correlated Visibility > Operations > Policy > Administration > Work-Centers

Authentication > Authorization > Profiling > Posture > Client Provisioning > Policy Elements

Dictionary > Conditions > Results

Network Device Profile: Cisco

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP)

Native Supplicant Provisioning: ACL Value: BYOD Portal (default)

Static IP/Host name/FQDN

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PERMIT_ALL_TRAFFIC
cisco-av-pair = ui-redirect-ad=portal
cisco-av-pair = ui-redirect=https://ip:port/portal/gateway?sessionId=SessionId&portal=0d56f6f0-6d90-11e5-979e-005056bf2f0a&action=nsp

Save Reset

新建授权 Profile - 1

- 新建授权 profile

Identity Services Engine

Home ▶ Context Visibility ▶ Operations ▶ Policy ▶ Administration ▶ Work Centers

Authentication Authorization Profiling Posture Client Provisioning ▶ Policy Elements

Dictionarys ▶ Conditions ▶ Results

▶ Authentication

▶ Authorization

Authorization Profiles

Downloadable ACLs

▶ Profiling

▶ Posture

▶ Client Provisioning

Standard Authorization Profiles

For Policy [X] go to Administration > System > Backup & Restore > Policy Export Page

Selected 0 | Total 7

Edit Add Duplicate Delete Show All

<input type="checkbox"/>	Name	Profile	Description
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you co
<input type="checkbox"/>	Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/>	Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
<input type="checkbox"/>	NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
<input type="checkbox"/>	Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/>	DenyAccess		Default Profile with access type as Access-Reject
<input type="checkbox"/>	PermitAccess		Default Profile with access type as Access-Accept

新建授权 Profile - 2

- 新建授权 profile, "internet_only"

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for creating a new Authorization Profile. The interface includes a navigation menu on the left and a main configuration area on the right. The main configuration area is titled "Authorization Profile" and contains the following fields and options:

- Name:** "internet_only" (highlighted with a red box and a circled '1')
- Description:** (empty text field)
- Access Type:** "ACCESS_ACCEPT" (dropdown menu)
- Network Device Profile:** "Cisco" (dropdown menu)
- Service Template:** (checkbox, unchecked)
- Track Movement:** (checkbox, unchecked)
- Passive Identity Tracking:** (checkbox, unchecked)
- Common Tasks:**
 - Web Authentication (Local Web Auth):** (checkbox, unchecked)
 - Airspace ACL Name:** (checkbox, checked) with a value of "internet_only" (highlighted with a red box and a circled '2')
 - ASA VPN:** (checkbox, unchecked)
 - A/C Profile Name:** (checkbox, unchecked)
- Advanced Attributes Settings:** (collapsible section, currently collapsed)
- Attributes Details:** (collapsible section, currently collapsed)

At the bottom of the page, there are "Submit" and "Cancel" buttons. The "Submit" button is highlighted with a red box and a circled '3'.

乾乾堂现任明教教主 CCIE Security

新建授权 Profile - 3

- 新建授权 profile, "permit_all"

The screenshot shows the Cisco ISE configuration interface for creating a new Authorization Profile. The interface is divided into a left sidebar and a main content area. The sidebar contains navigation options: Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. The main content area is titled "Authorization Profiles > New Authorization Profile" and contains the following fields and options:

- Name:** A text input field containing "permit_all", highlighted with a red box and a red circle with the number 1.
- Description:** An empty text input field.
- Access Type:** A dropdown menu set to "ACCESS_ACCEPT".
- Network Device Profile:** A dropdown menu set to "Cisco".
- Service Template:** A checkbox that is unchecked.
- Track Movement:** A checkbox that is unchecked.
- Passive Identity Tracking:** A checkbox that is unchecked.
- Common Tasks:** A section with several checkboxes:
 - Web Authentication (Local Web Auth)
 - Airespace ACL Name, with a text input field containing "permit_all", highlighted with a red box and a red circle with the number 2.
 - ASA VPN
 - A/C Profile Name
- Advanced Attributes Settings:** A section that is currently collapsed.
- Attributes Details:** A section that is currently collapsed.
- Buttons:** "Submit" and "Cancel" buttons at the bottom, with the "Submit" button highlighted by a red box and a red circle with the number 3.

创建 logical profile - 1

- 创建 logical profile

The screenshot shows the Cisco Identity Services Engine (ISE) Profiling page. The navigation menu includes Home, Context Visibility, Operations, Policy (selected), Administration, and Work Centers. The main menu includes Authentication, Authorization, Profiling (selected), Posture, Client Provisioning, and Policy Elements. The Profiling page displays a search bar, a left sidebar with 'Logical Profiles' selected, and a main content area with a table of Logical Profiles. The 'Add' button is highlighted with a red box and a circled '4'. The table lists various device types and their descriptions.

Logical Profiles	System Type	Description
<input type="checkbox"/> Cameras	Cisco Provided	Default logical profile for cameras.
<input type="checkbox"/> Gaming Devices	Cisco Provided	Default logical profile for gaming devices.
<input type="checkbox"/> Home Network Devices	Cisco Provided	Default logical profile for home network devices.
<input type="checkbox"/> IP-Phones	Administrator Modified	Default logical profile for IP Phones.
<input type="checkbox"/> Infrastructure Network Devices	Cisco Provided	Default logical profile for infrastructure network devices.
<input type="checkbox"/> Medical Devices	Cisco Provided	Default logical profile for medical devices.
<input type="checkbox"/> Mobile Devices	Cisco Provided	Default logical profile for mobile devices.
<input type="checkbox"/> Printers	Cisco Provided	Default logical profile for printers.

创建 logical profile - 2

- 创建 logical profile

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Profiling

Logical Profiles List > New Logical Profile

Logical Profile

* Name **1** apple_device Description

* Policy Assignment

Available Policies:

- 2Wire-Device
- 3Com-Device
- Aastra-Device
- Aastra-IP-Phone
- Aerohive-Access-Point
- Aerohive-Device
- American-Power-Conversion-Device
- Android

Assigned Policies:

- 2** Apple-Device

3 Submit Cancel

创建 logical profile - 3

- 创建 logical profile

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Profiling

Logical Profiles List > New Logical Profile

Logical Profile

* Name 1 Description

* Policy Assignment

Available Policies:

- 2Wire-Device
- 3Com-Device
- Aastra-Device
- Aastra-IP-Phone
- Aerohive-Access-Point
- Aerohive-Device
- American-Power-Conversion-Device
- Android-Amazon

Assigned Policies:

- Android 2

Submit 3 Cancel

乾颐堂 明教 CCIE Security

创建授权策略(1)

- 创建授权策略

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring Policy Sets. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' menu is highlighted with a red circle labeled '1'. Below the navigation bar, the 'Policy Sets' tab is highlighted with a red circle labeled '2'. The main content area shows a table of Policy Sets with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. A search bar is located below the table. The 'Default' policy set is highlighted with a red box labeled '3', specifically pointing to the 'Actions' column which contains a right-pointing arrow icon. The page also features 'Reset' and 'Save' buttons.

创建授权策略(2)

- 创建授权策略

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets → Default Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access +	0
➤ Authentication Policy (3)					
➤ Authorization Policy - Local Exceptions					
➤ Authorization Policy - Global Exceptions					
➤ Authorization Policy (10) 1					

Reset Save

创建授权策略(3)

- 创建授权策略

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
4	Employee_EAP-TLS_Android	Wireless_802.1X BYOD_is_Registered EAP-TLS MAC_in_SAN EndPoints-LogicalProfile EQUALS Android_device	internet_only	BYOD	0	Settings
3	Employee_EAP-TLS_Apple	Wireless_802.1X BYOD_is_Registered EAP-TLS MAC_in_SAN EndPoints-LogicalProfile EQUALS apple_device	internet_only	BYOD	0	Settings
2	Employee_EAP-TLS_PC	Wireless_802.1X BYOD_is_Registered EAP-TLS MAC_in_SAN	permit_all	BYOD	0	Settings
1	Employee_Onboarding	Wireless_802.1X EAP-MSCHAPV2	NSP_Onboard	BYOD	0	Settings

克隆(改名)+添加Endpoint条件

克隆(改名)+添加Endpoint条件+授权结果

激活默认+改名+授权结果

激活默认



乾頤堂 4.4 配置WLAN Security

WLC 上查看已经关联的 AP

- 查看 AP

The screenshot shows the Cisco WLC GUI. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS' (selected), 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar contains a tree view with 'Wireless' expanded and 'Access Points' selected. The main content area shows 'All APs' with a 'Current Filter' of 'None' and 'Number of APs' as '1'. A table lists the AP details:

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time	Admin Sta
APfc5b.3937.1a98	20.1.1.136	AIR-CAP1602I-C-K9	fc:5b:39:37:1a:98	0 d, 09 h 59 m 39 s	Enabled

WLC 上创建 Dynamic Interface - 1

- WLC 上创建 Dynamic Interface

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLAN', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'CONTROLLER' tab is selected and highlighted with a red box and a red circle containing the number '1'. On the left sidebar, the 'Interfaces' link is highlighted with a red box and a red circle containing the number '2'. In the top right corner, the 'New...' button is highlighted with a red box and a red circle containing the number '3'. The main content area displays a table of interfaces.

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	10	10.1.1.100	Static	Enabled	::/128
redundancy-management	10	0.0.0.0	Static	Not Supported	
redundancy-port	untagged	0.0.0.0	Static	Not Supported	
service-port	N/A	0.0.0.0	DHCP	Disabled	::/128
virtual	N/A	1.1.1.1	Static	Not Supported	

Entries 1 - 5 of 5 [New...](#)

WLC 上创建 Dynamic Interface - 2

- 创建 Dynamic Interface

The screenshot shows the Cisco WLC configuration page for creating a new dynamic interface. The breadcrumb path is "Interfaces > New". The "Interface Name" field contains "client" and the "VLAN Id" field contains "30". A red box highlights these two fields, with a red circle containing the number "1" next to it. In the top right corner, the "Apply" button is highlighted with a red box and a red circle containing the number "2". The "Back" button is also visible. The left sidebar shows the navigation menu with "Interfaces" selected. The top navigation bar includes "MONITOR", "WLANs", "CONTROLLER", "WIRELESS", "SECURITY", "MANAGEMENT", "COMMANDS", "HELP", and "FEEDBACK". The top right corner has links for "Save Configuration", "Ping", "Logout", and "Refresh".

Controller

- General
- Inventory
- Interfaces
- Interface Groups
- Multicast
- ▶ Network Routes
- ▶ Redundancy
- ▶ Internal DHCP Server
- ▶ Mobility Management
- Ports
- ▶ NTP
- ▶ CDP
- ▶ PMIPv6
- ▶ IPv6
- ▶ mDNS
- ▶ Advanced

Interfaces > New

Interface Name client

VLAN Id 30

< Back Apply

乾颐堂现任明教教主 CCIE Security

WLC 上创建 Dynamic Interface - 3

- 创建 Dynamic Interface

Controller: Interfaces > Edit

Save Configuration | Ping | Logout | Refresh

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

Controller: General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Redundancy, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, PMIPv6, IPv6, mDNS, Advanced

General Information

Interface Name: client
MAC Address: 58:8d:09:cd:b9:60

Configuration

Guest Lan:
Quarantine:
Quarantine Vlan Id: 0
NAS-ID: none

Physical Information

Port Number: 1
Backup Port: 0
Active Port: 0
Enable Dynamic AP Management:

Interface Address

VLAN Identifier: 30
IP Address: 30.1.1.253
Netmask: 255.255.255.0
Gateway: 30.1.1.254

DHCP Information

Primary DHCP Server: 30.1.1.254
Secondary DHCP Server:
DHCP Proxy Mode: Global
Enable DHCP Option 82:

< Back Apply

CCIE Security

WLC 上创建认证服务器 - 1

- 新建认证服务器



The screenshot shows the Cisco WLC configuration page for RADIUS Authentication Servers. The interface includes a top navigation bar with tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted with a red box and a '1' in a red circle), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the configuration tree with AAA > RADIUS > Authentication highlighted (marked with a '2' in a red circle). The main content area is titled 'RADIUS Authentication Servers' and contains the following configuration options:

- Auth Called Station ID Type: AP MAC Address:SSID
- Use AES Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- MAC Delimiter: Hyphen

At the bottom right, there are 'Apply' and 'New...' buttons, with 'New...' highlighted (marked with a '3' in a red circle). A table header is visible at the bottom of the configuration area:

Network User	Management	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
--------------	------------	--------------	---------------------------	------	-------	--------------

A large watermark 'CCIE Security' is overlaid on the right side of the interface.

WLC 上创建认证服务器 - 2

- 填写认证服务器信息

The screenshot displays the Cisco WLC configuration interface for RADIUS Authentication Servers. The configuration details are as follows:

Field	Value
Server Index	2
Server Address(Ipv4/Ipv6)	10.1.1.141
Shared Secret Format	ASCII
Shared Secret	...
Confirm Shared Secret	...
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for CoA	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	2 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
IPsec	<input type="checkbox"/> Enable

The 'Apply' button is highlighted with a red circle 4.

WLC 上创建授权服务器 - 1

- 新建审计服务器

Security

- AAA
 - General
 - RADIUS
 - 1 Accounting**
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
 - Local EAP
 - Advanced EAP
 - Priority Order
 - Certificate

RADIUS Accounting Servers

Acct Called Station ID Type: System MAC Address

MAC Delimiter: Hyphen

Network User

Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
--------------	---------------------------	------	-------	--------------

Apply **2** New...

CCIE Security

WLC 上创建授权服务器 - 2

- 编辑审计服务器信息

The screenshot displays the Cisco WLC configuration interface for RADIUS Accounting Servers. The left sidebar shows the navigation menu under 'Security' > 'AAA' > 'RADIUS' > 'Accounting'. The main content area is titled 'RADIUS Accounting Servers > Edit' and shows the configuration for a server with index 2. The configuration fields are as follows:

Field	Value
Server Index	2
Server Address(Ipv4/Ipv6)	10.1.1.141
Shared Secret Format	ASCII
Shared Secret	...
Confirm Shared Secret	...
Port Number	1813
Server Status	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Tunnel Proxy	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

Red circles with numbers 1, 2, and 3 highlight the 'Server Address', 'Shared Secret' field, and the 'Apply' button respectively. The 'Apply' button is located in the top right corner of the configuration area.

WLC 上创建 WLAN - 1

- 创建 WLAN

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes the Cisco logo and menu items: MONITOR, **WLANs** (highlighted with a red box and a '1' in a red circle), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The right side of the navigation bar has links for Save Configuration, Ping, Logout, and Refresh.

The main content area is titled 'WLANs' and shows 'Entries 0 - 0 of 0'. Below the title, there is a 'Current Filter: None' section with links for [Change Filter] and [Clear Filter]. To the right, there is a 'Create New' button (highlighted with a red box and a '3' in a red circle) and a 'Go' button.

On the left sidebar, there is a 'WLANs' section with a '2' in a red circle and a red box around it, and an 'Advanced' link below it.

A large watermark '乾颐堂现任明教教主 CCIE Security' is overlaid on the page.

WLC 上创建 WLAN - 2

- 创建 WLAN

WLANs > New

Type: WLAN

Profile Name: BYOD

SSID: BYOD

ID: 1

< Back Apply

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

- WLANs
- Advanced

乾颐堂现任明教教主 CCIE Security

WLC 上创建 WLAN - 3

- 编辑 WLAN

The screenshot shows the Cisco WLC configuration interface for editing a WLAN profile named 'BYOD'. The page is titled 'WLANs > Edit 'BYOD'' and has a navigation bar with tabs for 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. The 'General' tab is selected. The configuration fields are as follows:

- Profile Name:** BYOD
- Type:** WLAN
- SSID:** BYOD
- Status:** Enabled
- Security Policies:** [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
- Radio Policy:** All
- Interface/Interface Group:** client
- Multicast Vlan Feature:** Enabled
- Broadcast SSID:** Enabled
- NAS-ID:** 5508-1

Red boxes and numbers 1-5 highlight the following configuration steps:

1. The 'General' tab is selected.
2. The 'Profile Name' field is highlighted.
3. The 'Status' checkbox is highlighted.
4. The 'Interface/Interface Group' dropdown menu is highlighted.
5. The 'Broadcast SSID' checkbox is highlighted.

WLC 上创建 WLAN - 4

- 编辑 WLAN

The screenshot shows the Cisco WLC configuration page for editing a WLAN named 'BYOD'. The interface includes a navigation bar with 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' section is active, and the 'Security' tab is selected. The configuration is divided into several sections: 'Layer 2', 'Layer 3', and 'AAA Servers'. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. The 'Fast Transition' dropdown is set to 'Disable'. The 'Protected Management Frame' section shows 'PMF' set to 'Disabled'. The 'WPA+ WPA2 Parameters' section includes checkboxes for 'WPA Policy', 'WPA2 Policy', 'WPA2 Encryption' (with 'AES' selected), and 'OSEN Policy'. The 'Authentication Key Management' section shows '802.1X' checked and 'Enable' selected. The 'Apply' button is highlighted with a red circle and the number 6.

WLC 上创建 WLAN - 5

- 编辑 WLAN

The screenshot shows the Cisco WLC configuration page for editing a WLAN named 'BYOD'. The 'Security' tab is selected, and the 'AAA Servers' sub-tab is active. The 'Authentication Servers' section shows 'Server 1' configured with IP: 10.1.1.141 and Port: 1812. The 'Apply' button is highlighted.

WLANs > Edit 'BYOD'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface Enabled

Authentication Servers Enabled Accounting Servers Enabled EAP Parameters Enable

Server	Authentication Servers	Accounting Servers
Server 1	IP: 10.1.1.141, Port: 1812	IP: 10.1.1.141, Port: 1813
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

RADIUS Server Accounting

Interim Update Interim Interval 0 Seconds

WLC 上创建 WLAN - 6

- 编辑 WLAN

The screenshot shows the Cisco WLC configuration interface for editing a WLAN named 'BYOD'. The 'Advanced' tab is selected, and three red circles highlight specific settings:

- 1**: The 'Advanced' tab is selected.
- 2**: The 'Allow AAA Override' checkbox is checked and highlighted.
- 3**: The 'NAC State' dropdown menu is set to 'ISE NAC' and highlighted.

Other visible settings include:

- Coverage Hole Detection: Enabled
- Enable Session Timeout: 1800 (Session Timeout (secs))
- Aironet IE: Enabled
- Diagnostic Channel: Enabled
- Override Interface ACL: IPv4: None, IPv6: None
- Layer2 Ad: None
- URL ACL: None
- P2P Blocking Action: Disabled
- Client Exclusion: Enabled, 60 (Timeout Value (secs))
- Maximum Allowed Clients: 0
- Static IP Tunneling: Enabled
- Wi-Fi Direct Clients Policy: Disabled
- Maximum Allowed Clients Per AP Radio: 200
- DHCP: DHCP Server: Override, DHCP Addr. Assignment: Required
- OEAP: Split Tunnel: Enabled
- Management Frame Protection (MFP): MFP Client Protection: Optional
- DTIM Period (in beacon intervals): 802.11a/n (1 - 255): 1, 802.11b/g/n (1 - 255): 1
- NAC: NAC State: ISE NAC

AD 上创建 ISE 的 A 记录

- AD 上创建 ISE 的 A 记录

The screenshot shows the Windows DNS Manager interface. The left pane displays the DNS hierarchy for QYWIN2008, including the qytang.com zone. The main pane shows a list of DNS records, with the 'qytise2-master' record highlighted in red. A dialog box titled 'qytise2-master 属性' is open, showing the configuration for this record. The dialog has three numbered callouts: 1 points to the '主机 (A)' field containing 'qytise2-master', 2 points to the 'IP 地址 (P)' field containing '10.1.1.141', and 3 points to the 'qytise2-master' record in the main list.

名称	类型	数据	时间戳
(与父文件夹相同)	起始授权机构 (SOA)	[28], qytwin2008.qyta...	静态
(与父文件夹相同)	名称服务器 (NS)	qytwin2008.qytang.com.	静态
(与父文件夹相同)	主机 (A)	10.1.1.10	2018/3/14
qytise2-master	主机 (A)	10.1.1.141	静态
qytwin2008	主机 (A)	10.1.1.10	静态

qytise2-master 属性

主机 (A) | 安全

主机 (如果为空则使用其父域) (H):
qytise2-master 1

完全限定的域名 (FQDN) (F):
qytise2-master.qytang.com

IP 地址 (P):
10.1.1.141 2

更新相关的指针 (PTR)记录 (U)



5. BYOD测试

5.1 PC测试

5.2 安卓移动端测试

5.3 注册设备管理

乾颐堂现任助教教主 CCIE Security

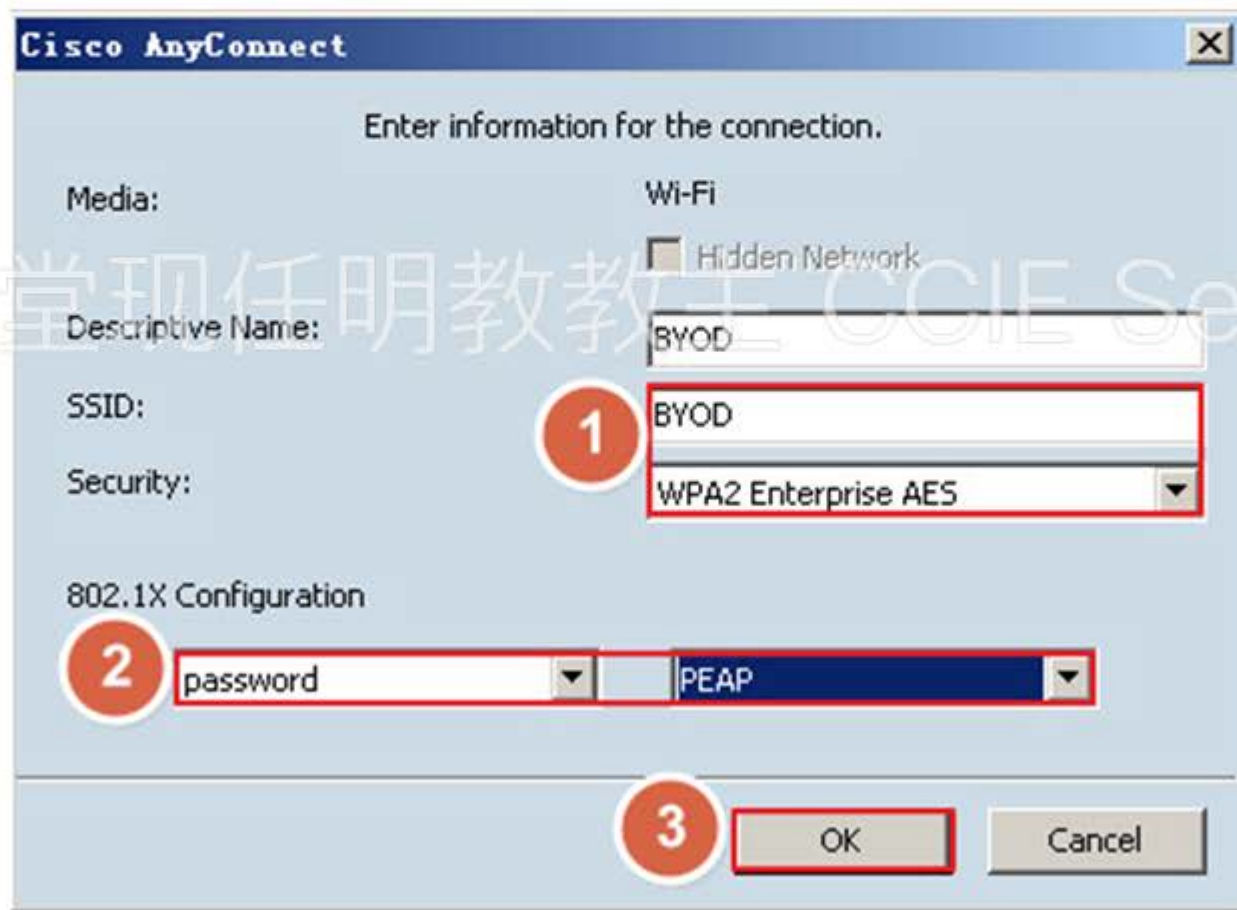


5.1 PC测试

乾颐堂现任明教教主 Qianyan Tang ISE Security

无线客户端连接测试 - 1

- 无线客户端使用 Anyconnect 连接 SSID “BYOD”，认证方式为“PEAP”

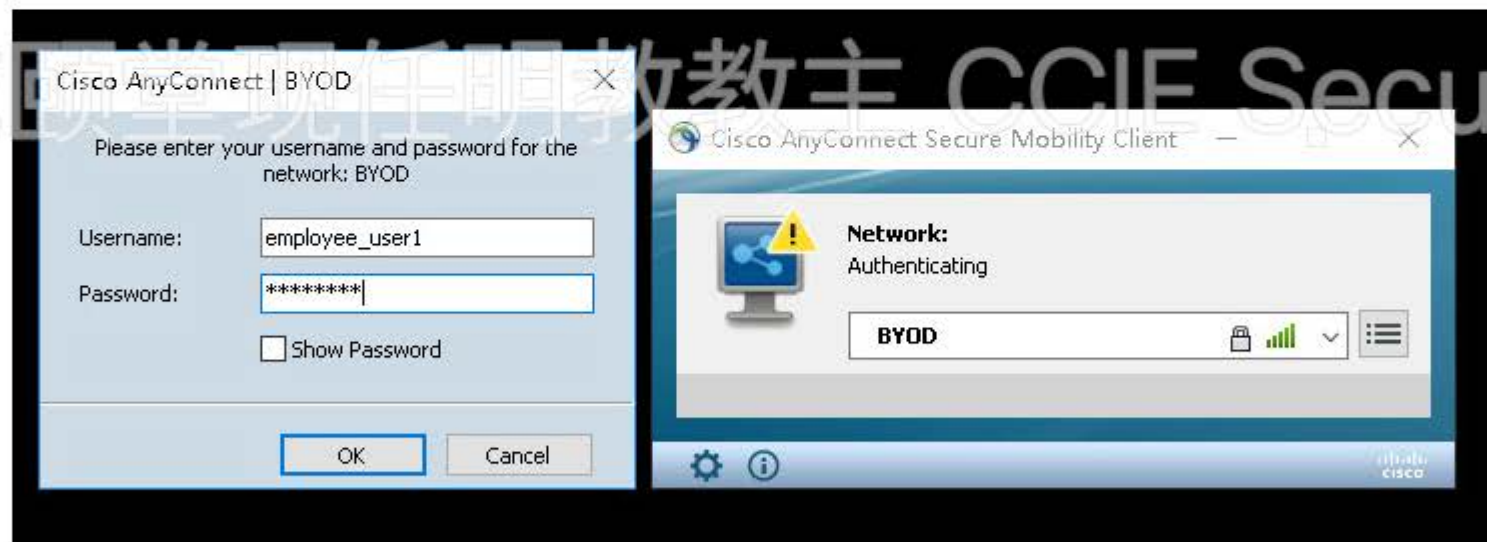


The screenshot shows the Cisco AnyConnect configuration window titled "Cisco AnyConnect". The main heading is "Enter information for the connection." The configuration is as follows:

- Media:** Wi-Fi
- Hidden Network
- Descriptive Name:** BYOD
- SSID:** BYOD (highlighted with a red box and a circled '1')
- Security:** WPA2 Enterprise AES
- 802.1X Configuration:**
 - Authentication Method: password (highlighted with a red box and a circled '2')
 - Authentication Protocol: PEAP (highlighted with a red box and a circled '2')
- Buttons:** OK (highlighted with a red box and a circled '3') and Cancel

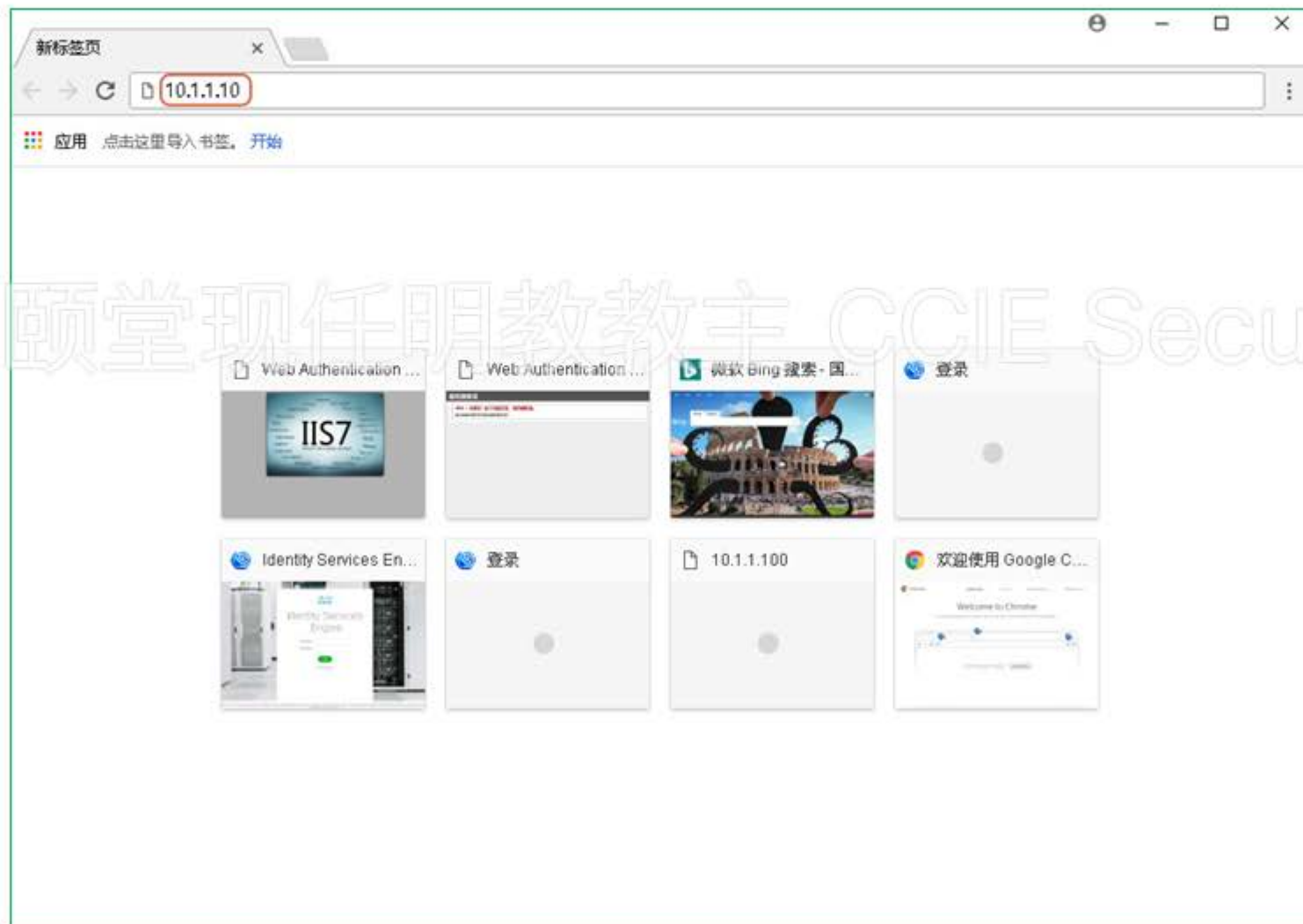
无线客户端连接测试 - 2

- 用 employee 账号测试



无线客户端连接测试 - 3

- 服务服务器地址，会被自动重定向



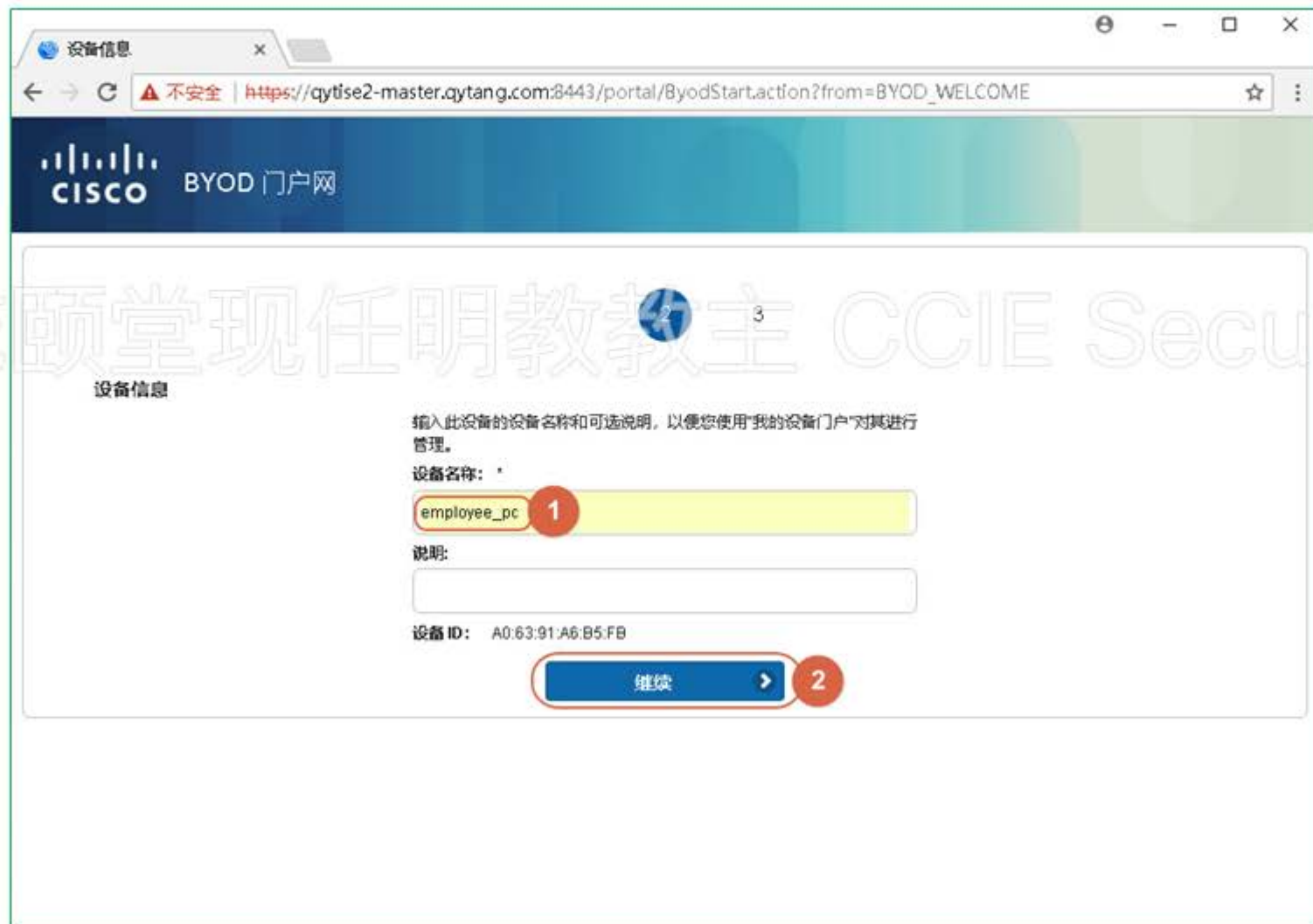
无线客户端连接测试 - 4

- 进入重定向页面



无线客户端连接测试 - 5

- 填写设备名称



设备信息

输入此设备的设备名称和可选说明，以便您使用“我的设备门户”对其进行管理。

设备名称: *

employee_pc 1

说明:

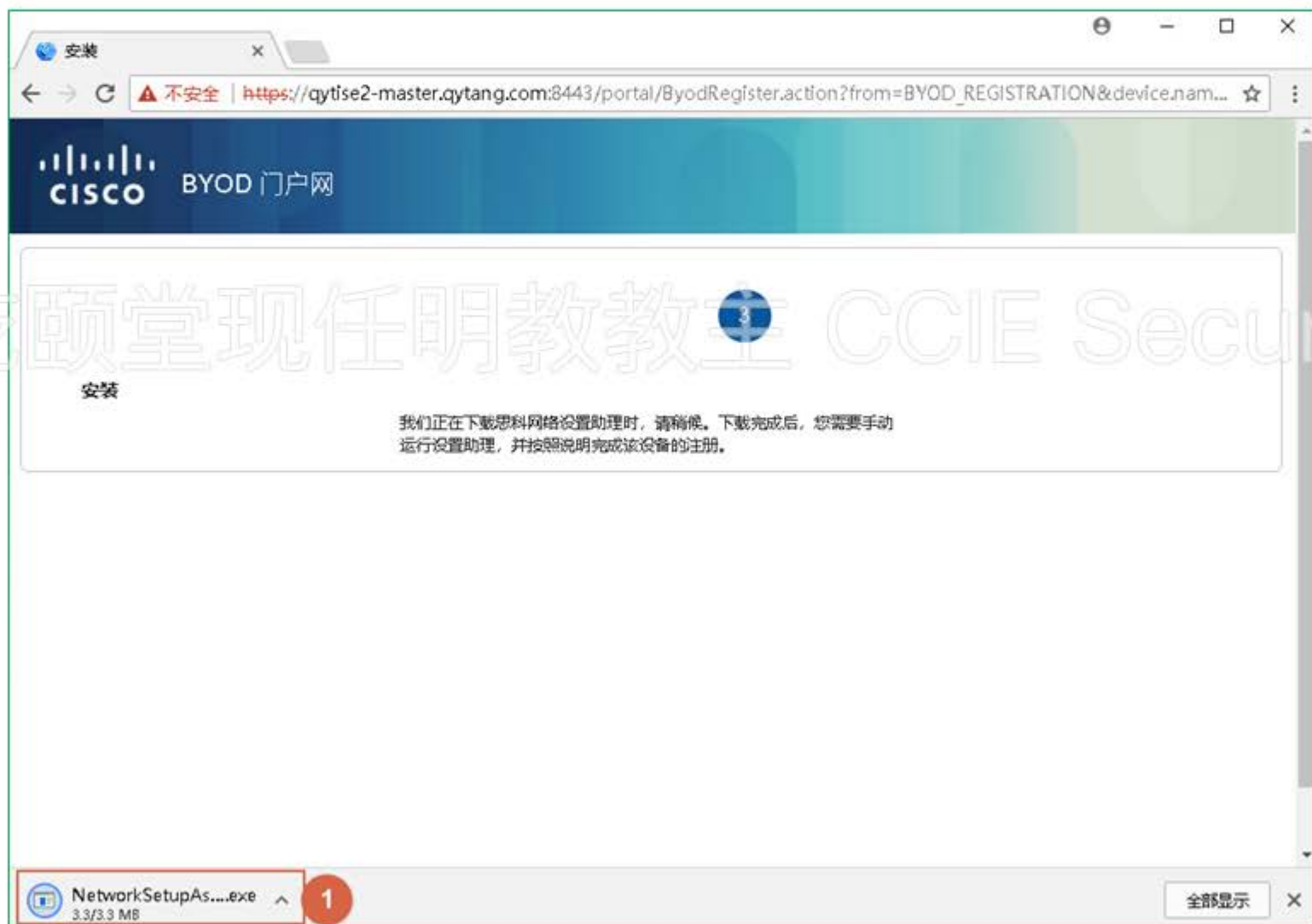
设备 ID: A0:63:91:A6:B5:FB

继续 > 2

乾颐堂现任明教教主 CCIE Security

无线客户端连接测试 - 6

- 下载软件



无线客户端连接测试 - 7

- 运行Network Setup Assistant



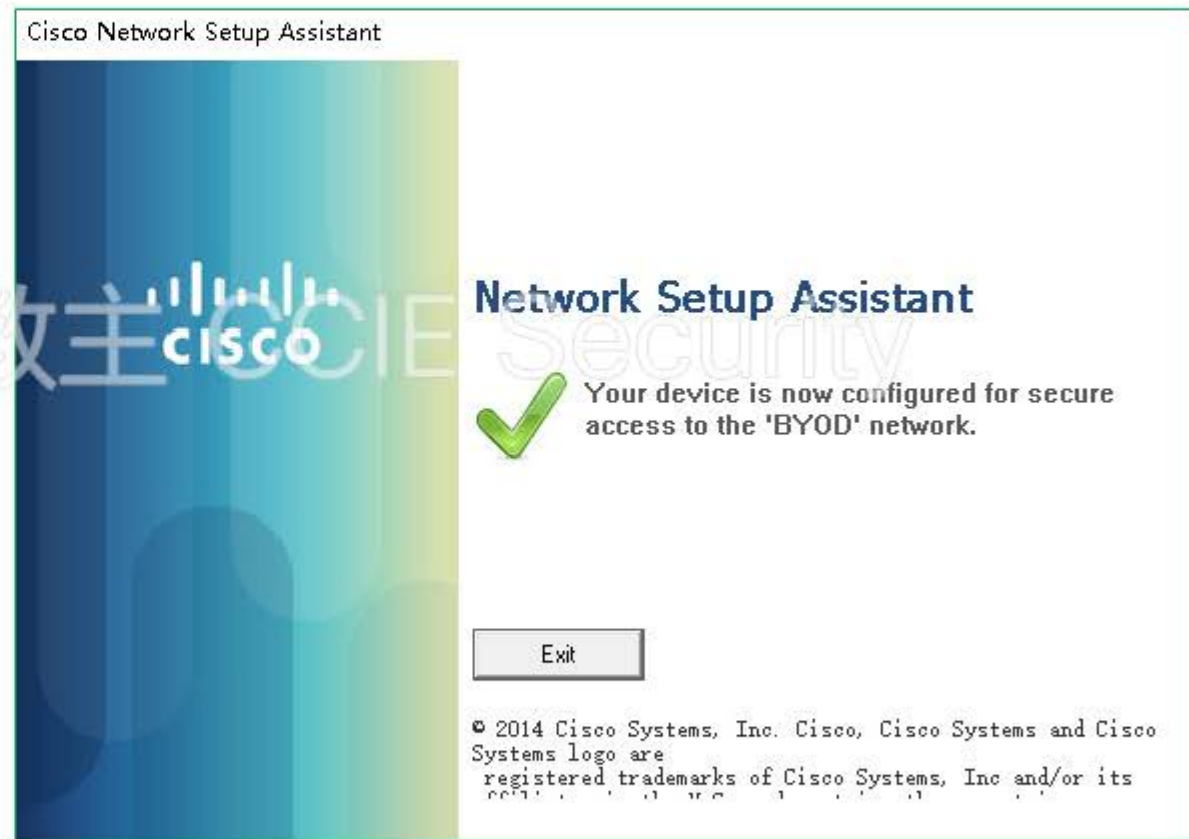
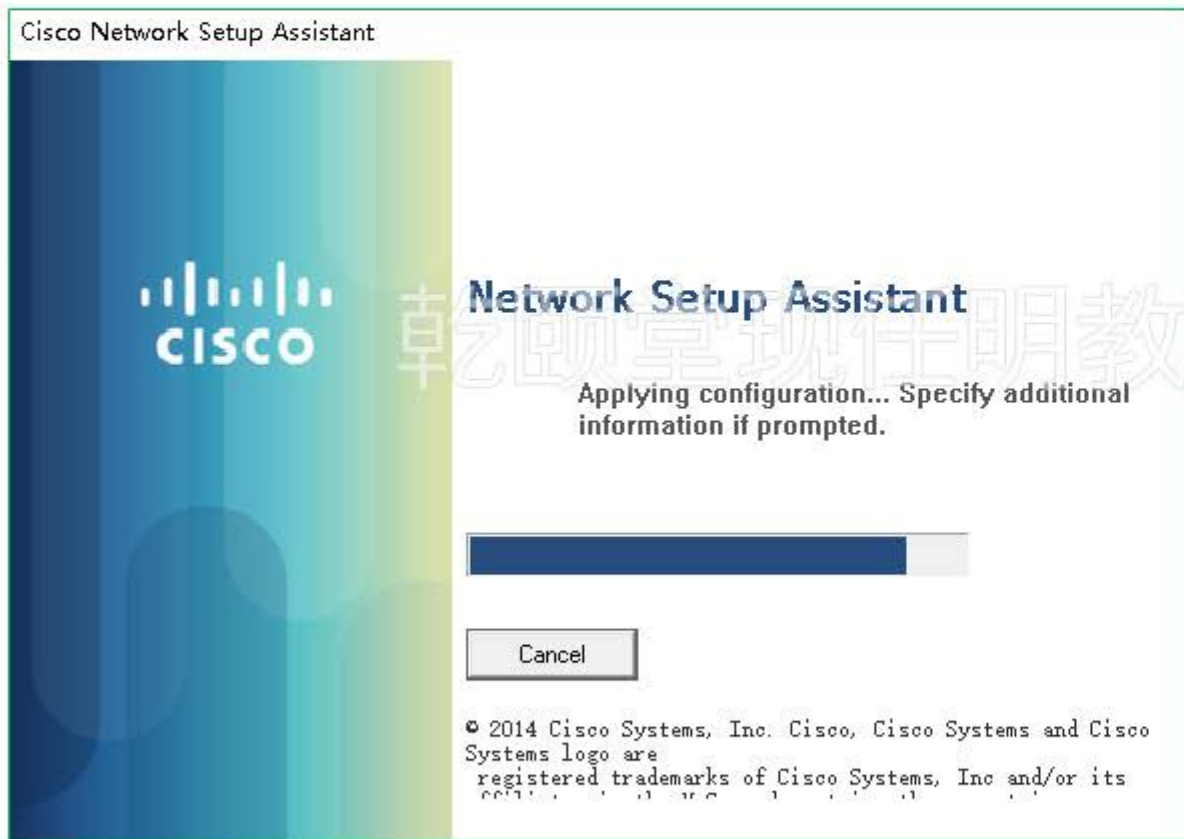
无线客户端连接测试 - 8

- 确认证书报错



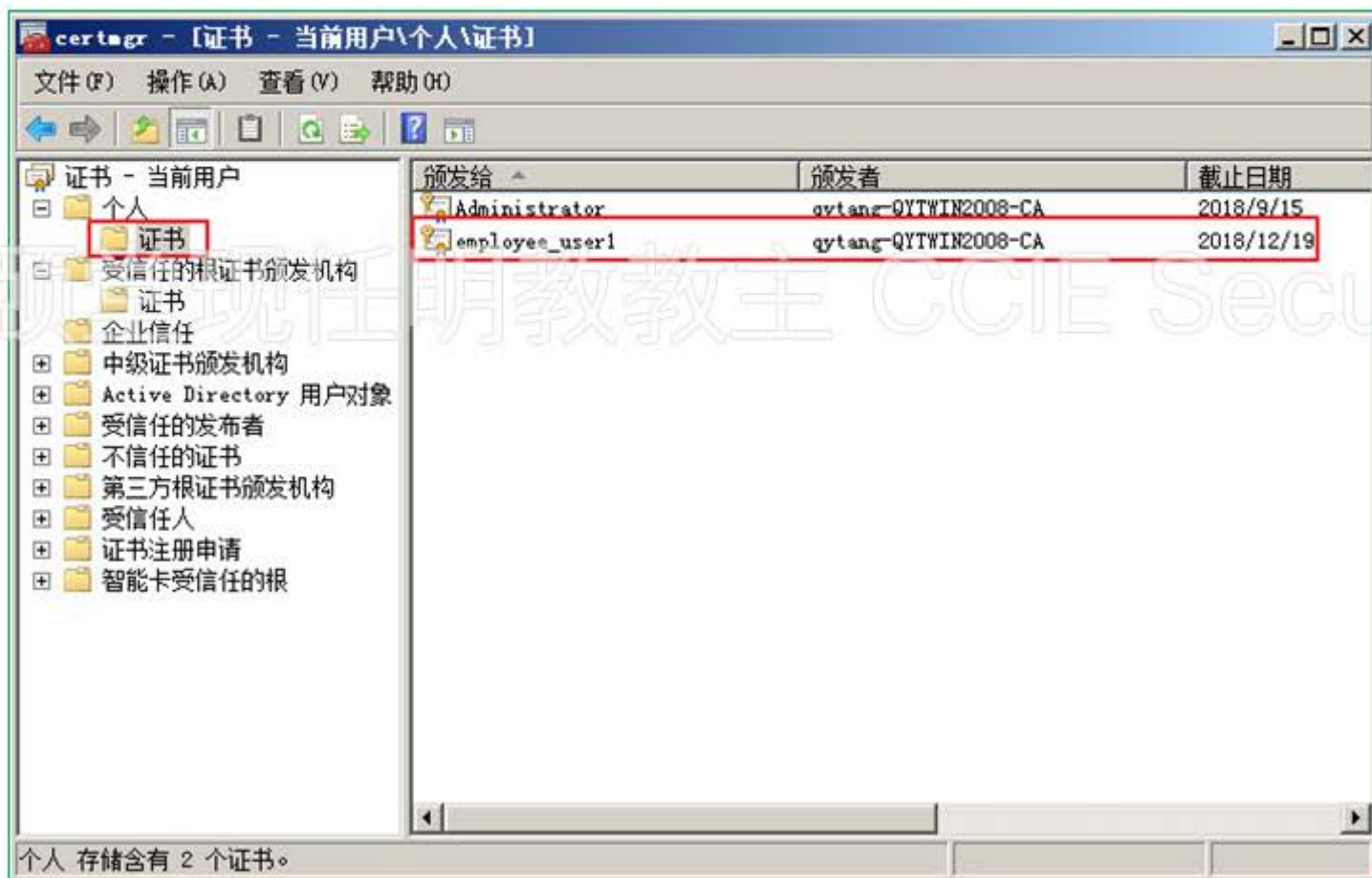
无线客户端连接测试 - 9

- 安装完毕

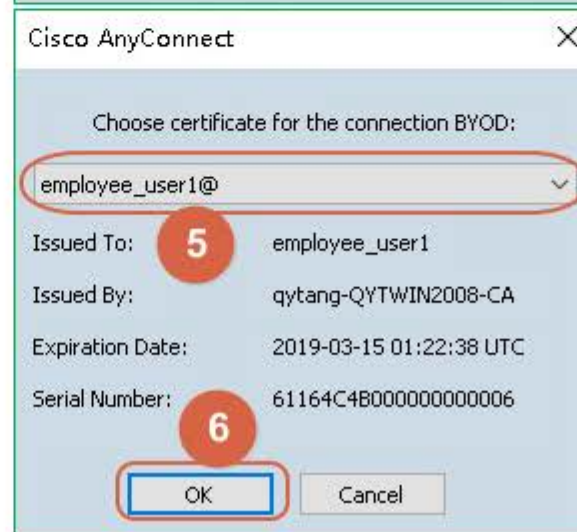
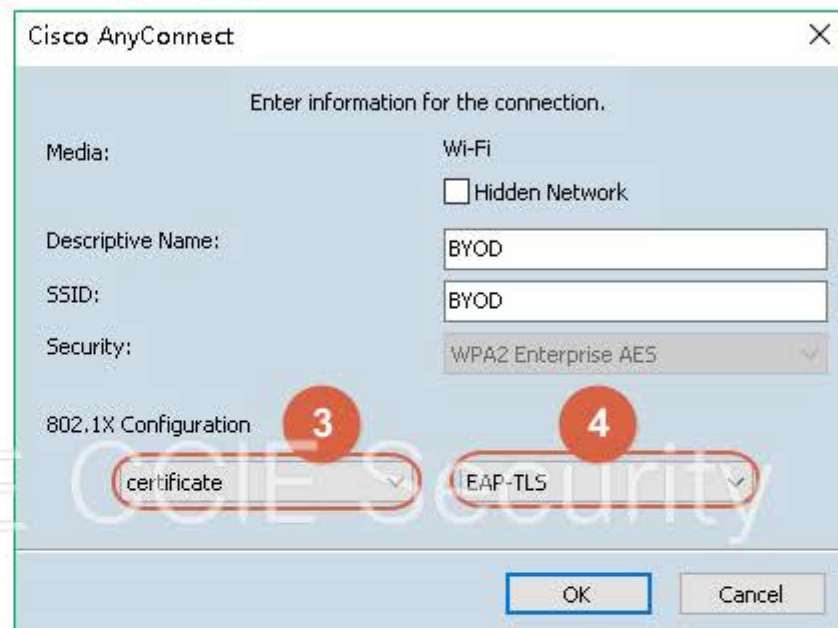


无线客户端查看个人证书

- 查看获取的个人证书



无线客户端使用证书认证



ISE 查看授权日志

- 查看授权结果变化

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

RADIUS Central-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 514 Client Stopped Responding 0 Repeat Counter 0

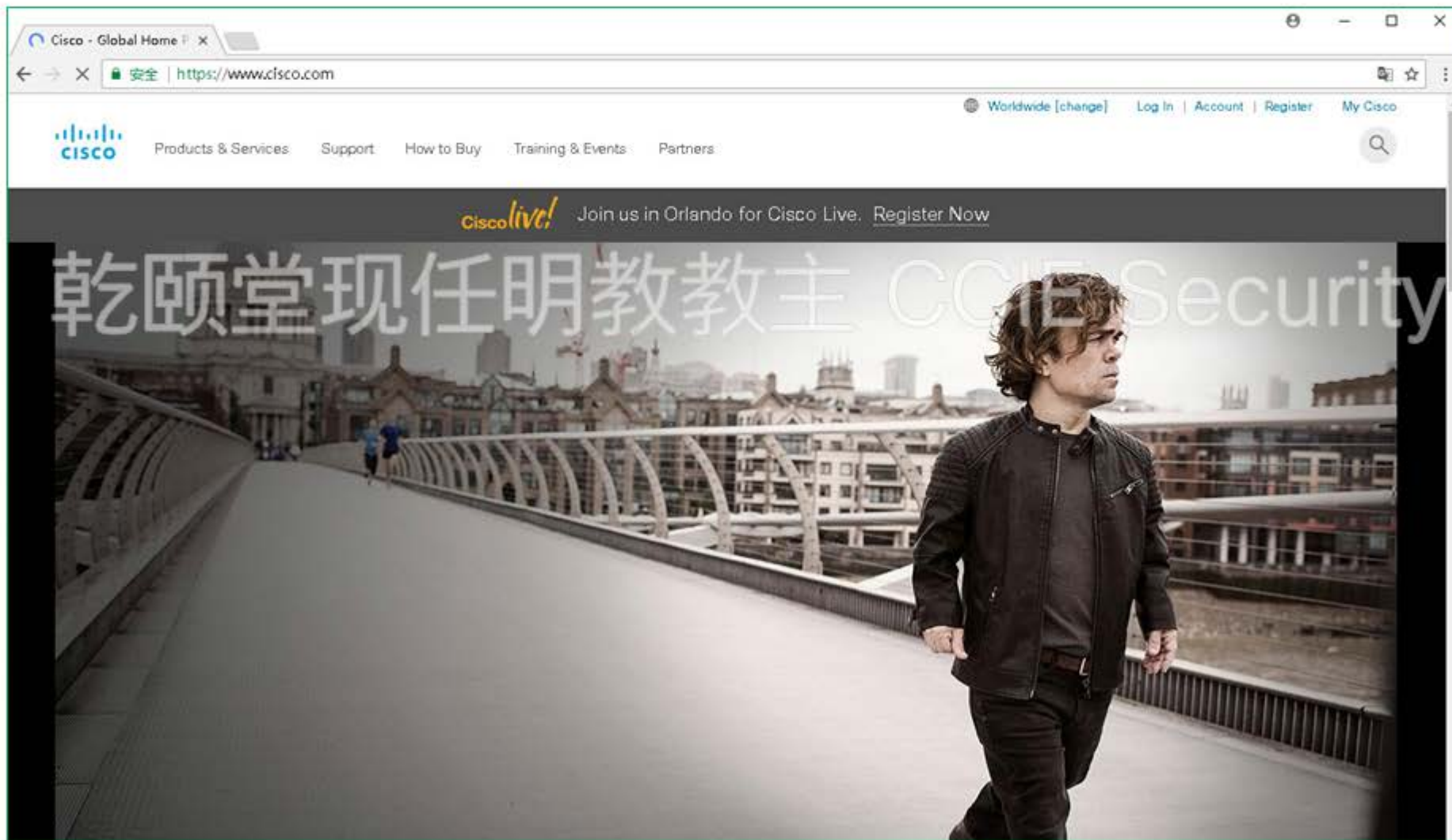
Refresh Never Show Latest 20 records Within Last 3 hours

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Profiles	IP Address
Mar 15, 2018 05:48:30.272 PM			0	employee_user1	A0:63:91:A6:B5:FB	Windows10...	Default >> D...	Default >> E...	BYOD,permit_all	30.1.1.1
Mar 15, 2018 05:48:30.248 PM				employee_user1	A0:63:91:A6:B5:FB	Windows10...	Default >> D...	Default >> E...	BYOD,permit_all	
Mar 15, 2018 05:43:57.815 PM				employee_user1	A0:63:91:A6:B5:FB	Windows10...	Default >> D...	Default >> E...	NSP_Onboard,BYOD	
Mar 15, 2018 05:43:51.489 PM				employee_user1	A0:63:91:A6:B5:FB	Windows10...	Default >> D...	Default >> E...	NSP_Onboard,BYOD	
Mar 15, 2018 05:43:50.160 PM				employee_user1	A0:63:91:A6:B5:FB	Windows10...	Default >> D...	Default >> E...	NSP_Onboard,BYOD	
Mar 15, 2018 05:43:43.700 PM				employee_user1	A0:63:91:A6:B5:FB	Windows10...	Default >> D...	Default >> E...	NSP_Onboard,BYOD	
Mar 15, 2018 05:36:40.210 PM				employee_user1	A0:63:91:A6:B5:FB	Netgear-Dev...	Default >> D...	Default >> E...	NSP_Onboard,BYOD	

无线客户端访问测试

- 授权结果是允许访问任意网络



WLC 查看授权列表

1 MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration Ping Logout Refresh Home

Monitor

Summary

- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
- Clients** 2
- Sleeping Clients
- Multicast
- Applications
- Lync
- Local Profiling

Clients > Detail

< Back Link Test Remove

Max Number of Records 10 Clear AVC Stats

Send CCX Req Display

General AVC Statistics

Group Tag	None Applied
AAA Override	
ACL Name	none
AAA Override	
ACL Applied	Unavailable
Status	
AAA Override	none
Flex ACL	
AAA Override	
Flex ACL Applied	Unavailable
Status	
Redirect URL	none
IPv4 ACL Name	permit_all 3
FlexConnect ACL Applied Status	Unavailable
IPv4 ACL Applied Status	Yes
IPv6 ACL Name	none
IPv6 ACL Applied Status	Unavailable
Layer2 ACL Name	none
Layer2 ACL Applied Status	Unavailable
URL ACL Name	none
URL ACL Applied Status	Unavailable
mDNS Status	Enabled
mDNS Profile Name	default-mdns-profile
mDNS Service Advertisement Count	0
AAA Role Type	none



5.2 安卓移动端测试

安卓测试 - 1



连接 BYOD



登录



开始

安卓测试 - 2



输入设备名称



转到 Google Play



点击 Cisco Network Setup

安卓测试 - 3



离开网页



转到 Google Play 去安装



打开软件

安卓测试 - 4



开始



继续



安装个人证书, 更改凭据用途

安卓测试 - 5



安装根证书，更改凭据用途



点击 BYOD

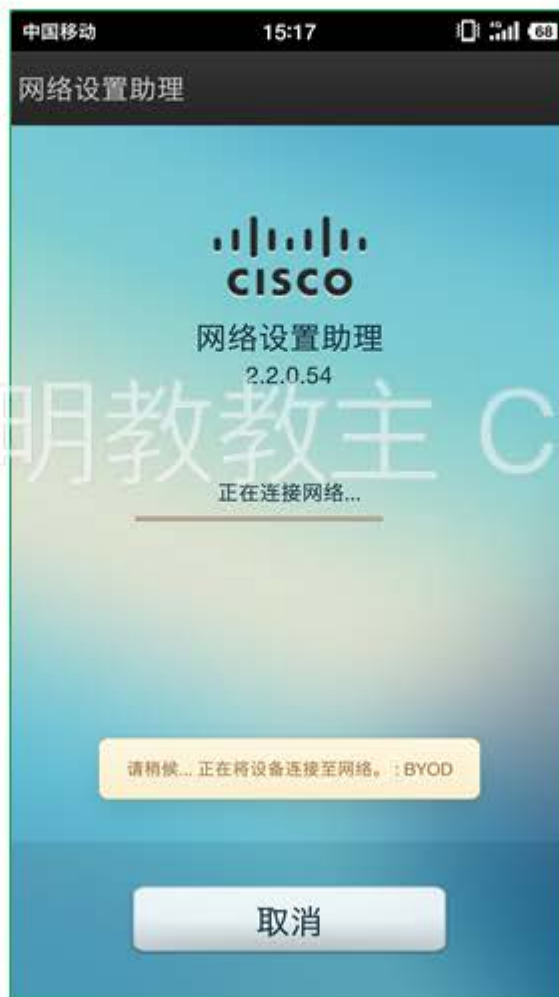


忘记此网络

安卓测试 - 6



返回



自动连接



连接成功，切换到浏览器

安卓测试 - 7



乾颐堂现任明教教主 CIE Security

测试访问权限



5.3 注册设备管理

修改授权 Profile - 1

Identity Services Engine

Home ▶ Context Visibility ▶ Operations **1** ▶ Policy ▶ Administration ▶ Work Centers

Authentication Authorization **2** Profiling Posture Client Provisioning ▶ Policy Elements

Dictionaryes ▶ Conditions **2** ▶ Results

3 Authorization

Authorization Profiles

Downloadable ACLs

▶ Profiling

▶ Posture

▶ Client Provisioning

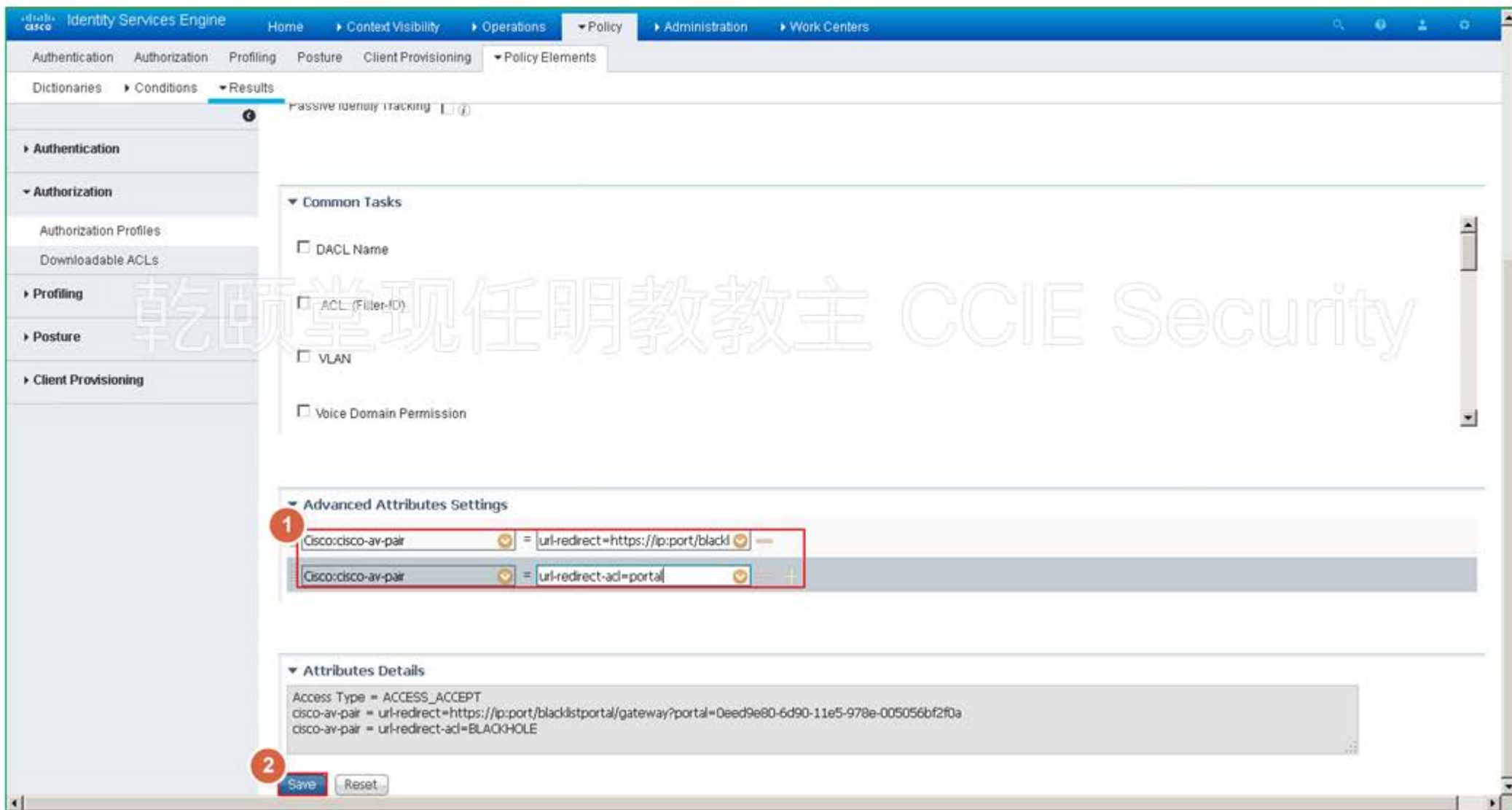
5 Edit + Add Duplicate Delete

Selected 0 | Total 9

Show All

Name	Profile	Description
4 Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE
<input type="checkbox"/> Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/> Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
<input type="checkbox"/> NSP_Onboard	Cisco	Onboard the device with Native Supplciant Provisioning
<input type="checkbox"/> Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/> internet_only	Cisco	
<input type="checkbox"/> permit_all	Cisco	
<input type="checkbox"/> DenyAccess		Default Profile with access type as Access-Reject
<input type="checkbox"/> PermitAccess		Default Profile with access type as Access-Accept

修改授权 Profile - 2



Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Passive identity tracking

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Common Tasks

DACL Name

ACL (Filter-ID)

VLAN

Voice Domain Permission

Advanced Attributes Settings

1 Cisco:cisco-av-pair = url-redirect=https://ip.port/black

Cisco:cisco-av-pair = url-redirect-ad=portal

Attributes Details

Access Type = ACCESS_ACCEPT

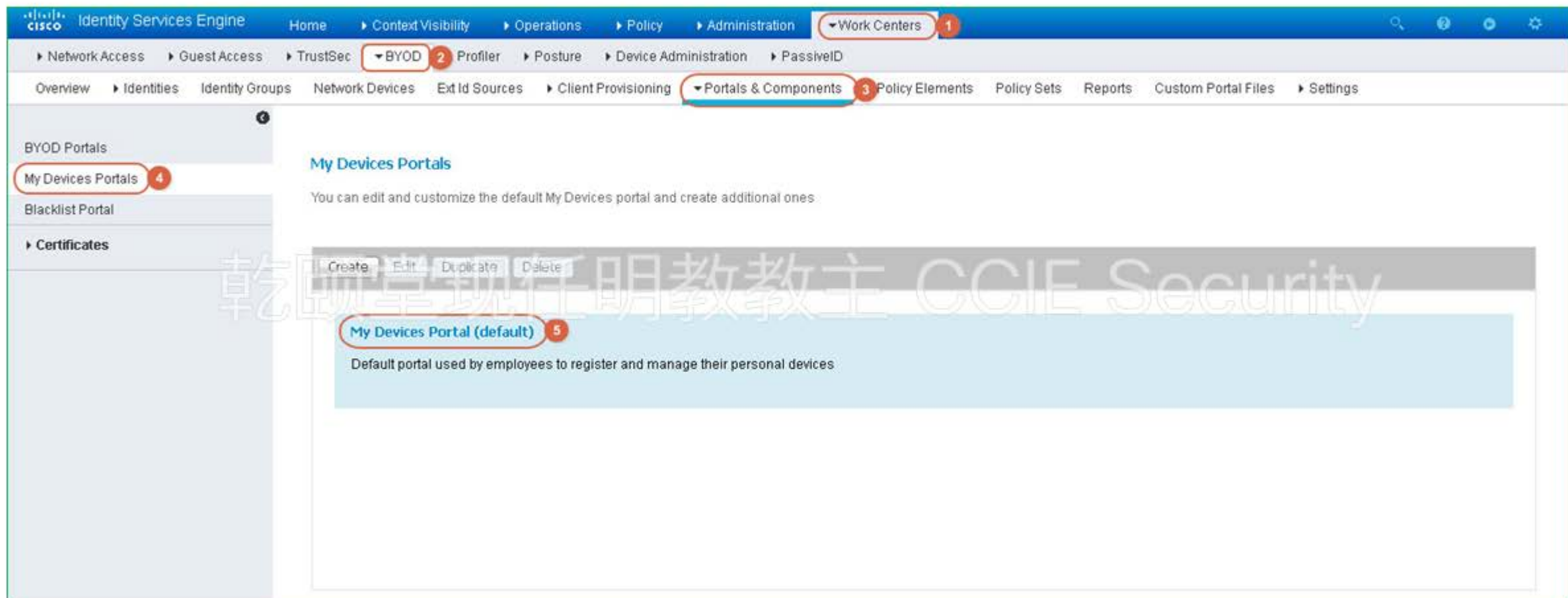
cisco-av-pair = url-redirect=https://ip.port/blacklistportal/gateway?portal=Deed9e80-6d90-11e5-978e-005056bf2f0a

cisco-av-pair = url-redirect-ad=BLACKHOLE

2 Save Reset

乾颐堂现任明教教主 CCIE Security

设置 Mydevice Portal - 1



The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for My Devices Portals. The interface includes a navigation menu on the left and a main content area. Red circles with numbers 1 through 5 highlight specific elements:

- 1: Work Centers menu item
- 2: BYOD menu item
- 3: Portals & Components menu item
- 4: My Devices Portals menu item in the left sidebar
- 5: My Devices Portal (default) entry in the main content area

The main content area displays the following text:

My Devices Portals

You can edit and customize the default My Devices portal and create additional ones

Buttons: Create, Edit, Duplicate, Delete

My Devices Portal (default) 5

Default portal used by employees to register and manage their personal devices

Watermark: 乾颐堂现任明教教主 CCIE Security

设置 Mydevice Portal - 2

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

Overview > Identities > Identity Groups > Network Devices > Ext Id Sources > Client Provisioning > Portals & Components > Policy Elements > Policy Sets > Reports > Custom Portal Files > Settings

BYOD Portals

My Devices Portals

Blacklist Portal

Certificates

Portal Behavior and Flow Settings
Use these settings to specify the guest experience for this portal.

Portal Page Customization
Customize portal pages by applying a theme and specifying field names and messages displayed to users.

Portal & Page Settings

My Devices Flow (Based on settings)

Portal Settings

HTTPS port: 9443 (9000 - 8999)

Allowed interfaces: Make selections in one or both columns based on your PSN configurations.

If bonding **is not** configured (i) on a PSN, use:

- Gigabit Ethernet 0
- Gigabit Ethernet 1
- Gigabit Ethernet 2
- Gigabit Ethernet 3
- Gigabit Ethernet 4
- Gigabit Ethernet 5

If bonding **is** configured (i) on a PSN, use:

- Bond 0
Uses Gigabit Ethernet 0 as primary, 1 as backup.
- Bond 1
Uses Gigabit Ethernet 2 as primary, 3 as backup.
- Bond 2
Uses Gigabit Ethernet 4 as primary, 5 as backup.

Certificate: Default Portal Certificate Group

group tag: Configure certificates at: Administration > System > Certificates > System Certificates

Fully qualified domain names: mydevice.qytang.com 1

(FQDN) and

Flow Diagram:

```

graph TD
    LOGIN[LOGIN] --> ALP[ALP]
    ALP --> Banner[Post Login Banner]
    Banner --> Home[My Devices Home]
  
```

授权策略

Identity Services Engine Home Context Visibility Operations **Policy** Administration Work Centers

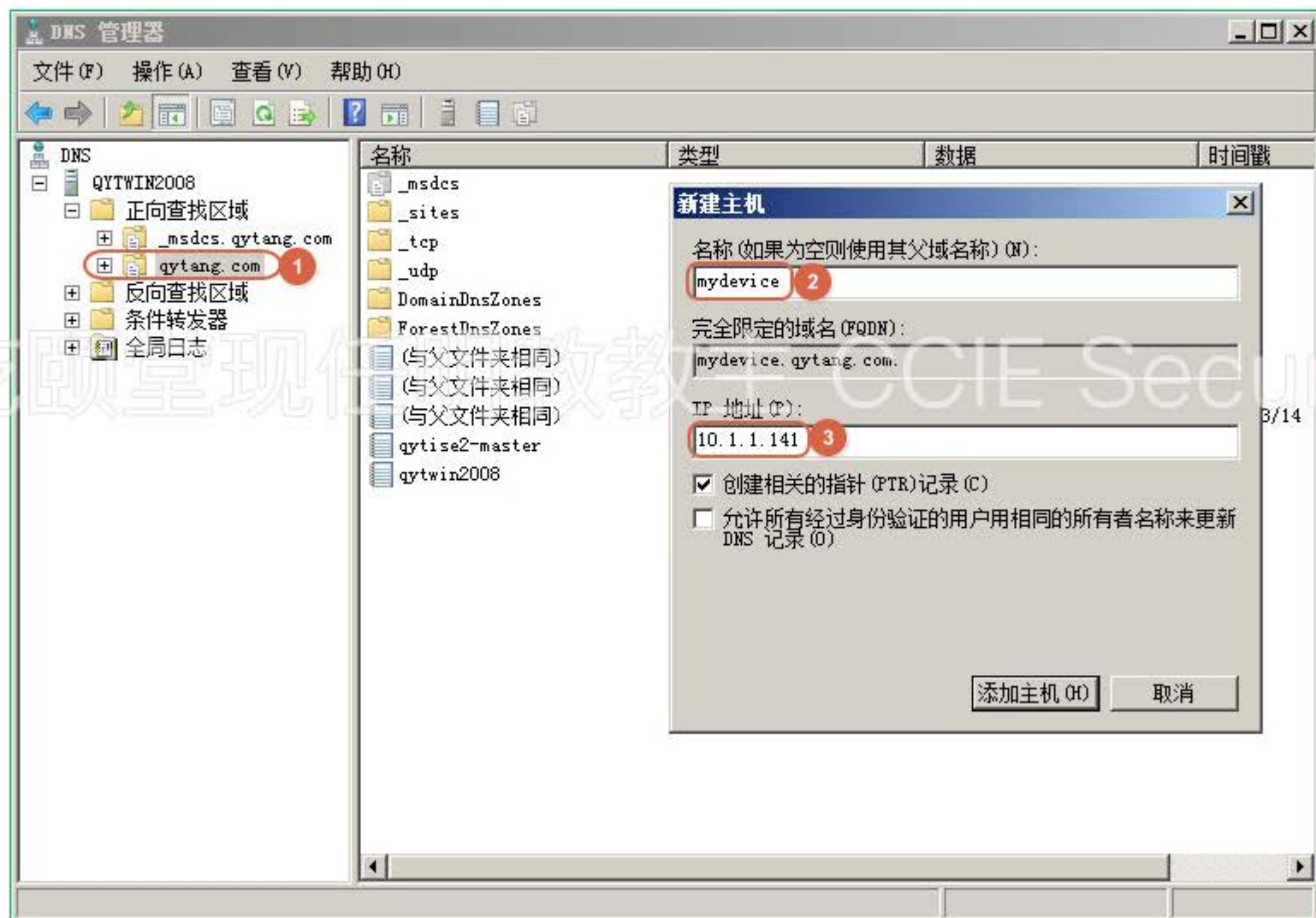
Policy Sets Profiling Posture Client Provisioning Policy Elements **1**

Policy Sets → Default **2** Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits		
✓	Default	Default policy set		Default Network Access x +	95		
<ul style="list-style-type: none"> Authentication Policy (3) Authorization Policy - Local Exceptions Authorization Policy - Global Exceptions 							
Authorization Policy (12) 3							
+ Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
Search							
4 ✓	Wireless Black List Default	AND	<ul style="list-style-type: none"> Wireless_Access IdentityGroup-Name STARTS_WITH Endpoint Identity Groups:Blacklist 	Blackhole_Wireless_Access +	Select from list +	2	⚙️
✓	Profiled Cisco IP Phones	IdentityGroup-Name STARTS_WITH Endpoint Identity Groups:Profiled:Cisco-IP-Phone		Cisco_IP_Phones +	Select from list +	0	⚙️
✓	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones		Non_Cisco_IP_Phones +	Select from list +	0	⚙️

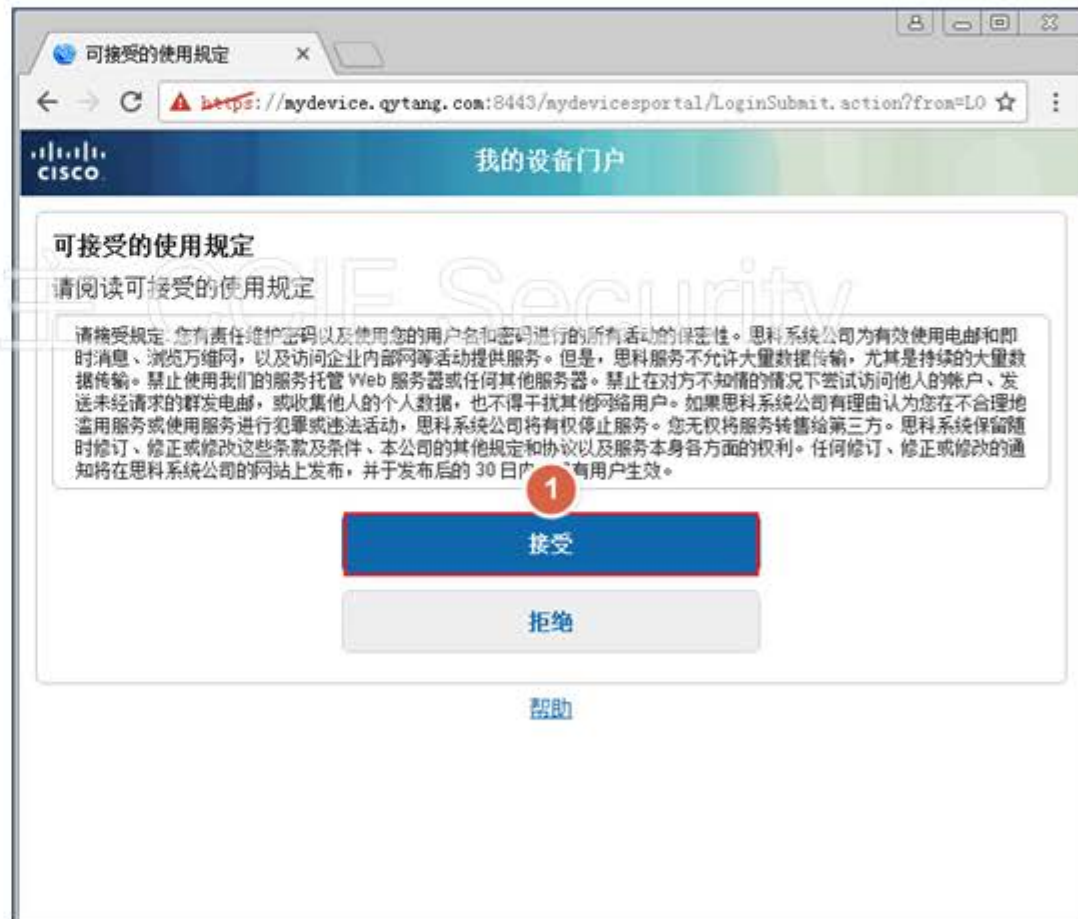
默认策略

AD 新建 DNS 映射



测试 Mydevice - 1

- 输入 <https://mydevice.qytang.com>



测试 Mydevice - 2

- 注册设备，点击进入设备



测试 Mydevice - 3

- 标记设备“已被盗”

管理设备
选择您要对设备执行的操作。

设备状态: Registered
设备名称: employee_pc
设备 ID: A0:63:91:A6:B5:FB
说明:

已丢失
已被盗 1
编辑
删除
关闭

如果您指示该设备被盗，则它将无法访问网络，直到您将其恢复。这可能需要近 2 分钟才能完成。是否继续？

是 否

帮助

测试 Mydevice - 4



CISCO 我的设备门户 欢迎 employee_user...

管理设备
需要添加设备吗？请选择添加。您的设备丢失或被盗了？请从列表中选择您的设备来管理它。

注册设备的数量：1/5

[添加](#) [刷新](#)

MAC Address

[已丢失](#) [已被盗](#) [物理](#) [PIN 锁定](#) [完全擦除](#) [注册](#) [设置](#) [删除](#)

MAC Address	Device Name	Description	Status
A0:63:91:A6:B5:FB	employee_pc		已被盗

[帮助](#)

测试 Mydevice - 5

- 由于设备“已被盗”访问服务器 10.1.1.10, 被阻止访问



测试 Mydevice - 6

- 授权已经切换到了Blackhole_Wireless_Access

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

RADIUS > Threat-Centric NAC Live Logs > TACACS > Troubleshoot > Adaptive Network Control > Reports

Live Logs > Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 514 Client Stopped Responding 0 Repeat Counter 0

Refresh Never Show Latest 20 records Within Last 3 hours

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Profiles	IP Address
Mar 15, 2018 06:13:30.158 PM	🔵	🔍	0	employee_user1	A0:63:91:A6:B5:FB	Windows10-...	Default >> D...	Default >> ...	Blackhole_Wireless_Access	30.1.1.1
Mar 15, 2018 06:13:30.095 PM	🟢	🔍		employee_user1	A0:63:91:A6:B5:FB	Windows10-...	Default >> D...	Default >> ...	Blackhole_Wireless_Access	
Mar 15, 2018 06:13:28.586 PM	🟢	🔍			A0:63:91:A6:B5:FB					
Mar 15, 2018 05:48:30.248 PM	🟢	🔍		employee_user1	A0:63:91:A6:B5:FB	Windows10-...	Default >> D...	Default >> E...	BYOD,permit_all	
Mar 15, 2018 05:43:57.815 PM	🟢	🔍		employee_user1	A0:63:91:A6:B5:FB	Windows10-...	Default >> D...	Default >> E...	NSP_Onboard,BYOD	
Mar 15, 2018 05:43:51.489 PM	🟢	🔍		employee_user1	A0:63:91:A6:B5:FB	Windows10-...	Default >> D...	Default >> E...	NSP_Onboard,BYOD	

测试 Mydevice - 7

- 管理 mydevice(继续访问https://mydevice.qytang.com)



测试 Mydevice - 8

- 恢复设备

The screenshot shows the Cisco Mydevice portal interface. At the top left is the Cisco logo and the text "我的设备门户". At the top right, there is a user greeting "欢迎 employee_user...". The main content area is titled "管理设备" (Manage Device) and includes the instruction "选择您要对设备执行的操作。" (Select the operation you want to perform on the device). Below this, a device information card displays the following details:

设备状态:	Stolen
设备名称:	employee_pc
设备 ID:	A0:63:91:A6:B5:FB
说明:	

Below the device information card, there are four buttons: "恢复" (Restore), "编辑" (Edit), "删除" (Delete), and "关闭" (Close). The "恢复" button is highlighted with a red circle and a red "1" in a circle next to it. At the bottom center, there is a "帮助" (Help) link.

查看 ISE 授权变化

- 恢复后设备获取到“permit_all”的授权

Identity Services Engine

Home | Context Visibility | Operations | Policy | Administration | Work Centers

RADIUS | Threat-Centric NAC Live Logs | TACACS | Troubleshoot | Adaptive Network Control | Reports

Live Logs | Live Sessions

Misconfigured Supplicants: 0 | Misconfigured Network Devices: 0 | RADIUS Drops: 514 | Client Stopped Responding: 0 | Repeat Counter: 0

Refresh | Reset Repeat Counts | Export To | Filter | Settings

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Profiles	IP Address
Mar 15, 2018 06:18:14.168 PM			0	employee_user1	A0:63:91:A6:B5:FB	Windows10...	Default >> D...	Default >> E...	BYOD,permit_all	30.1.1.1
Mar 15, 2018 06:18:14.054 PM				employee_user1	A0:63:91:A6:B5:FB	Windows10...	Default >> D...	Default >> E...	BYOD,permit_all	
Mar 15, 2018 06:18:12.585 PM					A0:63:91:A6:B5:FB					
Mar 15, 2018 06:13:30.095 PM				employee_user1	A0:63:91:A6:B5:FB	Windows10...	Default >> D...	Default >> ...	Blackhole_Wireless_Access	
Mar 15, 2018 06:13:28.586 PM					A0:63:91:A6:B5:FB					
Mar 15, 2018 05:48:30.248 PM				employee_user1	A0:63:91:A6:B5:FB	Windows10...	Default >> D...	Default >> E...	BYOD,permit_all	
Mar 15, 2018 05:43:57.815 PM				employee_user1	A0:63:91:A6:B5:FB	Windows10...	Default >> D...	Default >> E...	NSP_Onboard,BYOD	
Mar 15, 2018 05:43:51.489 PM				employee_user1	A0:63:91:A6:B5:FB	Windows10...	Default >> D...	Default >> E...	NSP_Onboard,BYOD	
Mar 15, 2018 05:43:50.160 PM					A0:63:91:A6:B5:FB					
Mar 15, 2018 05:43:43.700 PM				employee_user1	A0:63:91:A6:B5:FB	Windows10...	Default >> D...	Default >> E...	NSP_Onboard,BYOD	
Mar 15, 2018 05:36:40.210 PM				employee_user1	A0:63:91:A6:B5:FB	Netgear-Dev...	Default >> D...	Default >> E...	NSP_Onboard,BYOD	

客户端访问互联网

- 设备能够正常访问互联网

