

Wireless BYOD with Identity Services Engine

Document ID: 113476

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Topology
- Conventions

Wireless LAN Controller RADIUS NAC and CoA Overview

Wireless LAN Controller RADIUS NAC and CoA Feature Flow

ISE Profiling Overview

Create Internal Identity Users

Add Wireless LAN Controller to ISE

Configure ISE for Wireless Authentication

Bootstrap Wireless LAN Controller

- Connecting WLC to a Network

Add Authentication Servers (ISE) to WLC

Create WLC Employee Dynamic Interface

Create WLC Guest Dynamic Interface

Add 802.1x WLAN

Test WLC Dynamic Interfaces

Wireless Authentication for iOS (iPhone/iPad)

Add Posture Redirect ACL to WLC

Enable Profiling Probes on ISE

Enable ISE Profile Policies for Devices

ISE Authorization Profile for Posture Discovery Redirect

Create ISE Authorization Profile for Employee

Create ISE Authorization Profile for Contractor

Authorization Policy for Device Posture/Profiling

Testing Posture Remediation Policy

Authorization Policy for Differentiated Access

Testing CoA for Differentiated Access

WLC Guest WLAN

Testing the Guest WLAN and Guest Portal

ISE Wireless Sponsored Guest Access

Sponsoring Guest

Testing Guest Portal Access

Certificate Configuration

Windows 2008 Active Directory Integration

Add Active Directory Groups

Add Identity Source Sequence

ISE Wireless Sponsored Guest Access with Integrated AD

Configure SPAN on the Switch

Reference : Wireless Authentication for Apple MAC OS X

Reference : Wireless Authentication for Microsoft Windows XP

Reference: Wireless Authentication for Microsoft Windows 7

Related Information

Introduction

Cisco Identity Services Engine (ISE) is Cisco's next-generation policy server that provides authentication and authorization infrastructure to the Cisco TrustSec solution. It also provides two other critical services:

- The first service is to provide a way to profile endpoint device type automatically based on attributes Cisco ISE receives from various information sources. This service (called Profiler) provides equivalent functions to what Cisco has previously offered with the Cisco NAC Profiler appliance.
- Another important service that Cisco ISE provides is to scan endpoint compliance; for example, AV/AS software installation and its definition file validity (known as Posture). Cisco has been previously providing this exact posture function only with the Cisco NAC Appliance.

Cisco ISE provides an equivalent level of functionality, and it is integrated with 802.1X authentication mechanisms.

Cisco ISE integrated with wireless LAN controllers (WLCs) can provide profiling mechanisms of mobile devices such as Apple iDevices (iPhone, iPad, and iPod), Android-based smartphones, and others. For 802.1X users, Cisco ISE can provide the same level of services such as profiling and posture scanning. Guest services on Cisco ISE can also be integrated with the Cisco WLC by redirecting web authentication requests to Cisco ISE for authentication.

This document introduces the wireless solution for Bring Your Own Device (BYOD), such as providing differentiated access based on known endpoints and the user policy. This document does not provide the complete solution of BYOD, but serves to demonstrate a simple use case of dynamic access. Other configuration examples include using the ISE sponsor portal, where a privileged user can sponsor a guest for provisioning wireless guest access.

Prerequisites

Requirements

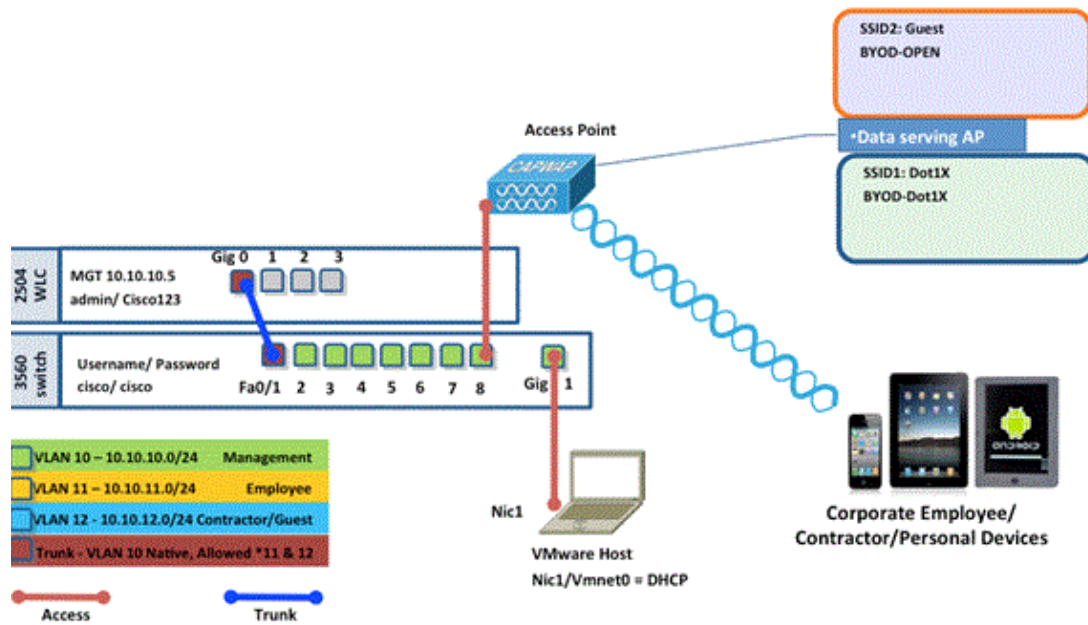
There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Wireless LAN Controller 2504 or 2106 with software version 7.2.103
- Catalyst 3560 8 ports
- WLC 2504
- Identity Services Engine 1.0MR (VMware server image version)
- Windows 2008 Server (VMware image) 512M, 20GB disk
 - ◆ Active Directory
 - ◆ DNS
 - ◆ DHCP
 - ◆ Certificate Services

Topology



Name	IP Address	Credential
Vmware Host	10.10.10.2	(Machine used to host the ISE 1.0 MR vmware server files)
Identity Service Engine	10.10.10.70	admin/ default1A
Active Directory/ DNS/ DHCP/ CA Server	10.10.10.10	(Machine used to host Active Directory/ DNS/ DHCP/ CA Server)

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Wireless LAN Controller RADIUS NAC and CoA Overview

This setting enables the WLC to look for the URL redirection AV-Pairs coming from the ISE RADIUS server. This is only on a WLAN that is tied to an interface with the RADIUS NAC setting enabled. When the Cisco AV-Pair for URL Redirection is received, the client is put into the POSTURE_REQD state. This is basically the same as the WEBAUTH_REQD state internally in the controller.

When the ISE RADIUS server deems the Client is Posture_Compliant, it issues a CoA ReAuth. The Session_ID is used to tie it together. With this new AuthC (re-Auth) it does not send the URL-Redirec AV-Pairs. Because there are no URL Redirect AV-Pairs, the WLC knows the client does not require Posture any longer.

If the RADIUS NAC setting is not enabled, the WLC ignores the URL Redirect VSA s.

CoA-ReAuth: This is enabled with the RFC 3576 Setting. ReAuth capability was added to the existing CoA commands that were supported previously.

The RADIUS NAC setting is mutually exclusive from this capability, although it is required for the CoA to work.

Pre-Posture ACL: When a client is in POSTURE_REQ state, the default behavior of the WLC is to block all traffic except DHCP/DNS. The Pre-Posture ACL (which it is called in the url-redirect-acl AV-Pair) is applied to the client, and what is permitted in that ACL is what the client can reach.

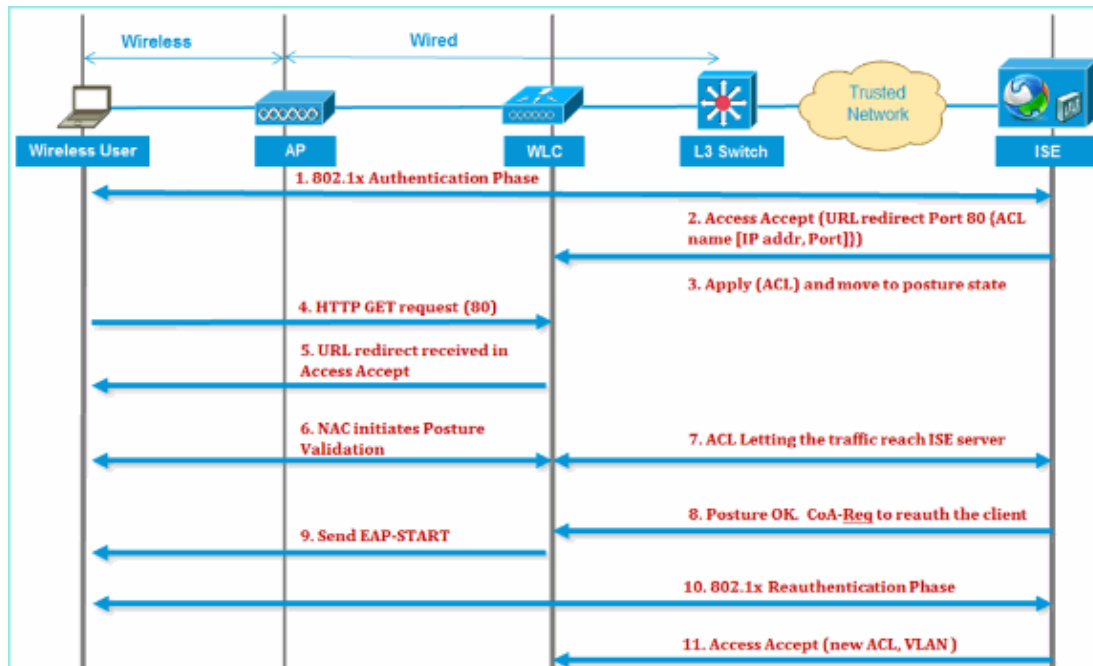
Pre-Auth ACL vs. VLAN Override: A Quarantine or AuthC VLAN that is different from the Access-VLAN is not supported in 7.0MR1. If you set a VLAN from the Policy Server, it will be the VLAN for the entire session. No VLAN changes are needed after first AuthZ.

Wireless LAN Controller RADIUS NAC and CoA Feature Flow

The below figure provides details of the message exchange when the client is authenticated to the backend server and NAC posture validation.

1. Client authenticates using dot1x authentication.
2. RADIUS Access Accept carries redirected URL for port 80 and pre-auth ACLs that includes allowing IP addresses and ports, or quarantine VLAN.
3. Client will be re-directed to the URL provided in access accept, and put into a new state until posture validation is done. The client in this state talks to the ISE server and validate itself against the policies configured on the ISE NAC server.
4. NAC agent on client initiates posture validation (traffic to port 80): Agent sends HTTP discovery request to port 80 which controller redirects to URL provided in access accept. The ISE knows that client trying to reach and responds directly to client. This way the client learns about the ISE server IP and from now on, the client talks directly with the ISE server.
5. WLC allows this traffic because the ACL is configured to allow this traffic. In case of VLAN override, the traffic is bridged so that it reaches the ISE server.
6. Once ISE-client completes assessment, a RADIUS CoA-Req with reauth service is sent to the WLC. This initiates re-authentication of the client (by sending EAP-START). Once re-authentication succeeds, the ISE sends access accept with a new ACL (if any) and no URL redirect, or access VLAN.
7. WLC has support for CoA-Req and Disconnect-Req as per RFC 3576. The WLC needs to support CoA-Req for re-auth service, as per RFC 5176.
8. Instead of downloadable ACLs, pre-configured ACLs are used on the WLC. The ISE server just sends the ACL name, which is already configured in controller.
9. This design should work for both VLAN and ACL cases. In case of VLAN override, we just redirect the port 80 is redirected and allows (bridge) rest of the traffic on the quarantine VLAN. For the ACL, the pre-auth ACL received in access accept is applied.

This figure provides a visual representation of this feature flow:



ISE Profiling Overview

Cisco ISE profiler service provides the functionality in discovering, locating, and determining the capabilities of all the attached endpoints on your network, regardless of their device types, in order to ensure and maintain appropriate access to your enterprise network. It primarily collects an attribute or a set of attributes of all the endpoints on your network and classifies them according to their profiles.

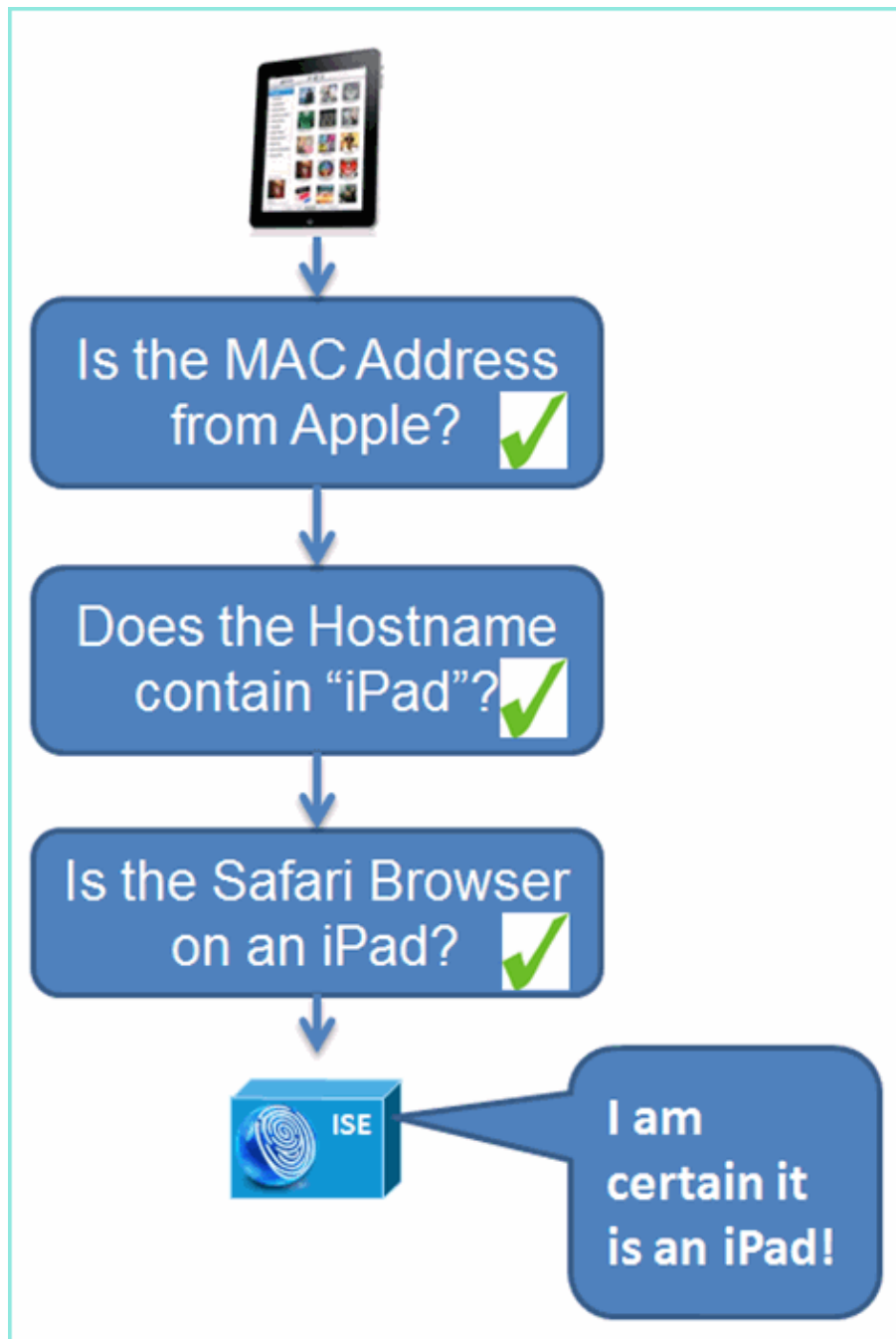
The profiler is comprised of these components:

- The sensor contains a number of probes. The probes capture network packets by querying network access devices, and forward the attributes and their attribute values that are collected from the endpoints to the analyzer.
- An analyzer evaluates endpoints using the configured policies and the identity groups to match the attributes and their attribute values collected, which classifies endpoints to the specified group and stores endpoints with the matched profile in the Cisco ISE database.

For mobile device detection, it is recommend to use a combination of these probes for proper device identification:

- RADIUS (Calling-Station-ID): Provides the MAC Address (OUI)
- DHCP (host-name): Hostname default hostname can include device type; for example: jsmith-ipad
- DNS (reverse IP lookup): FQDN – default hostname can include device type
- HTTP (User-Agent): Details on specific mobile device type

In this example of an iPad, the profiler captures the web browser information from the User-Agent attribute, as well as other HTTP attributes from the request messages, and adds them to the list of endpoint attributes.



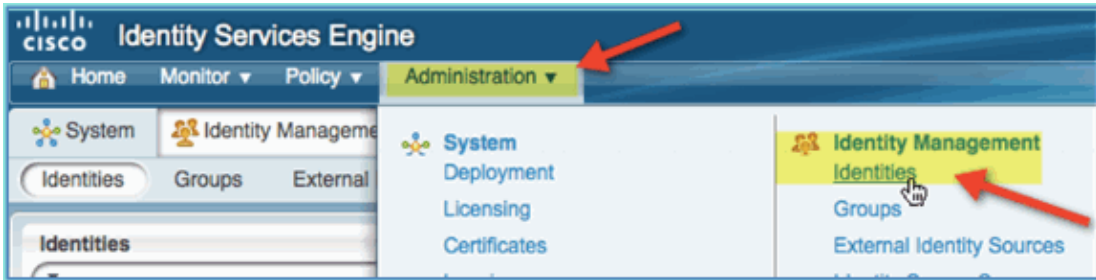
Create Internal Identity Users

MS Active Directory (AD) is not required for a simple proof-of-concept. ISE can be used as the sole identity store, which includes differentiating users access for access and granular policy control.

At the release of ISE 1.0, using AD integration, the ISE can use AD groups in authorization policies. If ISE internal user store is used (no AD integration), groups cannot be used in policies in conjunction with device identity groups (identified bug to be resolved in ISE 1.1). Therefore, only individual users can be differentiated, such as employees or contractors when used in addition to device identity groups.

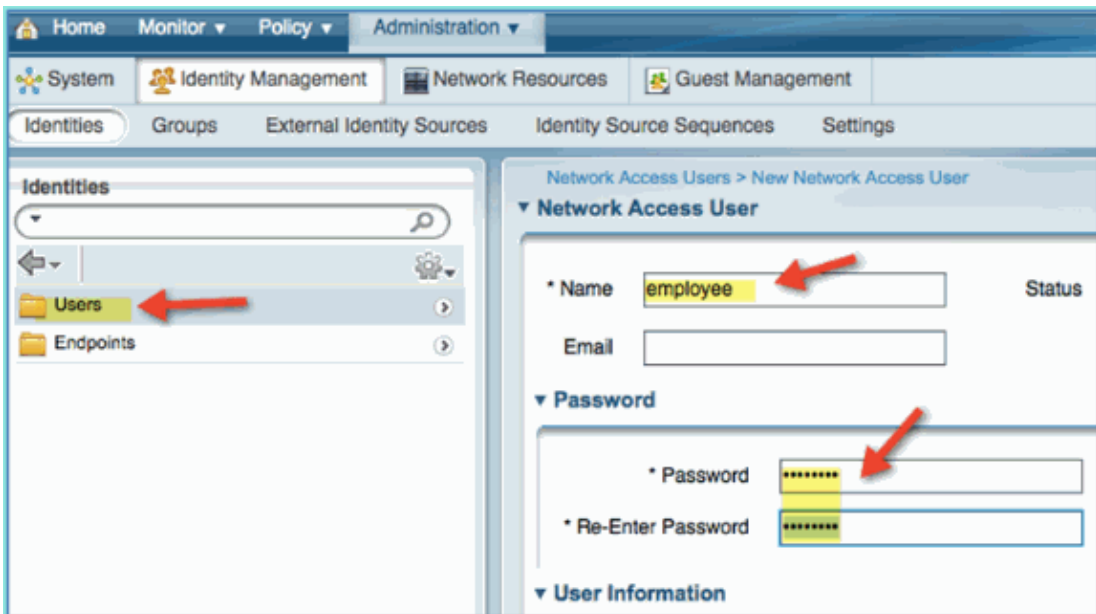
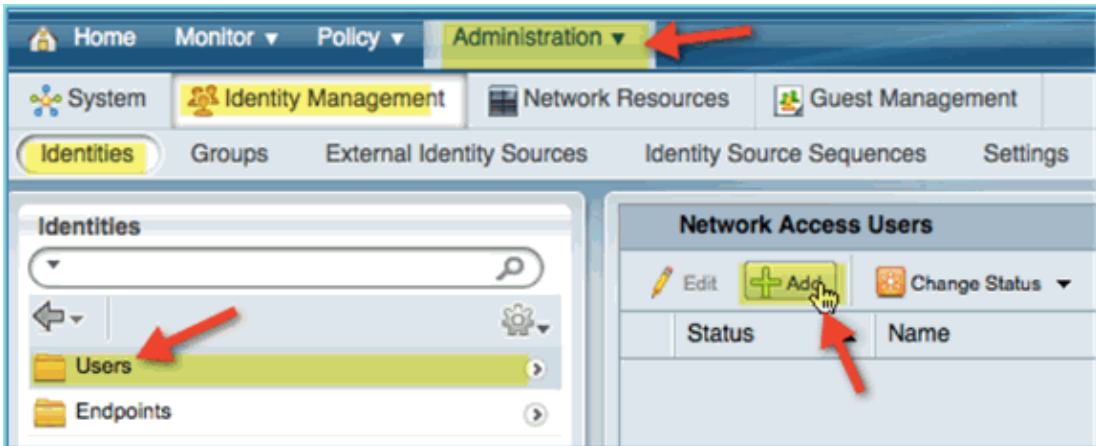
Complete these steps:

1. Open a browser window to the <https://ISEip> address.
2. Navigate to **Administration > Identity Management > Identities**.



3. Select **Users**, then click **Add** (Network Access User). Enter these user values and assign to Employee group:

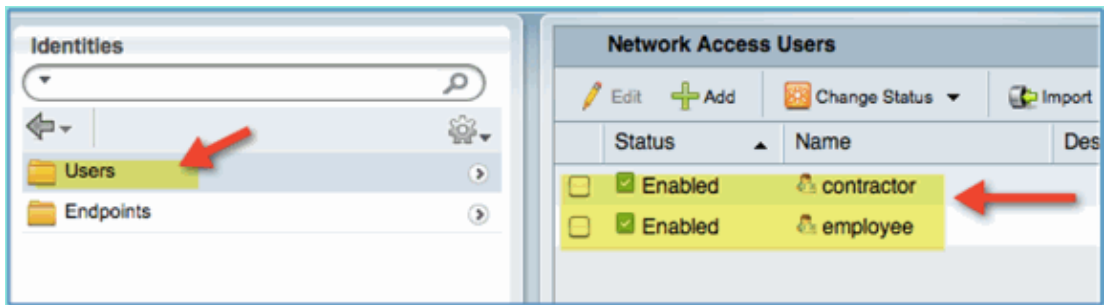
- ◆ Name: employee
- ◆ Password: XXXX



4. Click **Submit**.

- ◆ Name: contractor
- ◆ Password: XXXX

5. Confirm both accounts are created.



Add Wireless LAN Controller to ISE

Any device that initiates RADIUS requests to the ISE must have a definition in ISE. These network devices are defined based on their IP address. ISE network device definitions can specify IP address ranges thus allowing the definition to represent multiple actual devices.

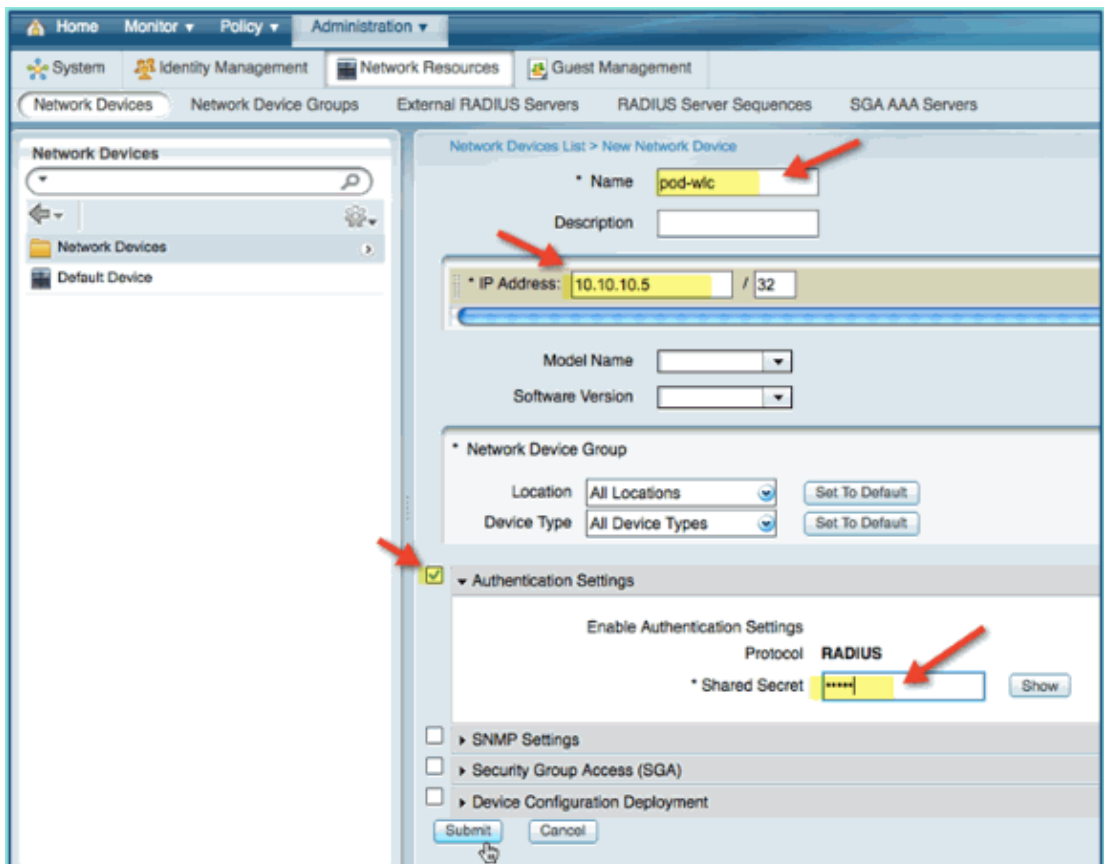
Beyond what is required for RADIUS communication, ISE network device definitions contain settings for other ISE/device communication, such as SNMP and SSH.

Another important aspect of network device definition is appropriately grouping devices so that this grouping can be leveraged in network access policy.

In this exercise, the device definitions required for your lab are configured.

Complete these steps:

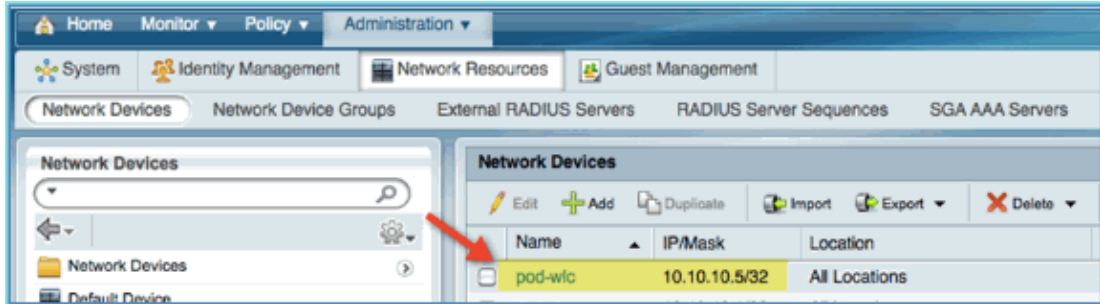
1. From ISE go to **Administration > Network Resources > Network Devices**.



2. From Network Devices, click **Add**. Enter IP address, mask check Authentication Setting, then enter

cisco for shared secret.

3. Save the WLC entry, and confirm controller on the list.

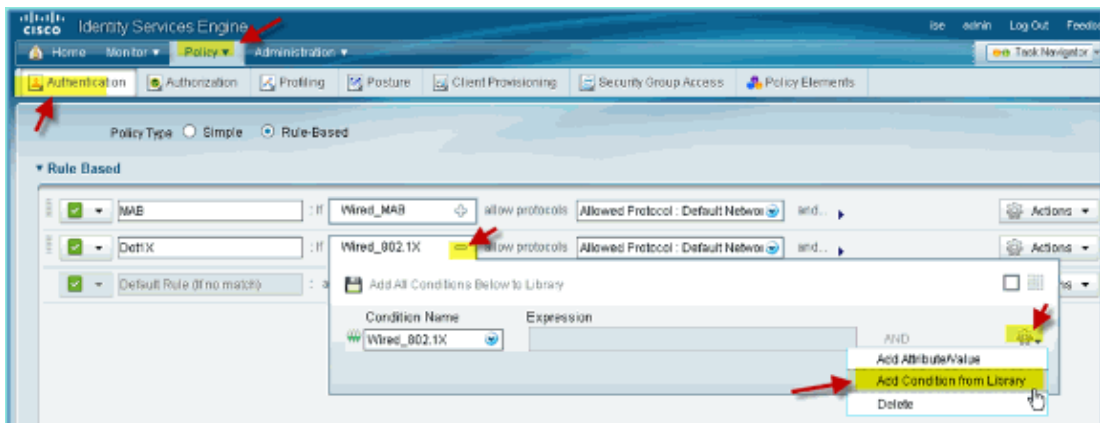


Configure ISE for Wireless Authentication

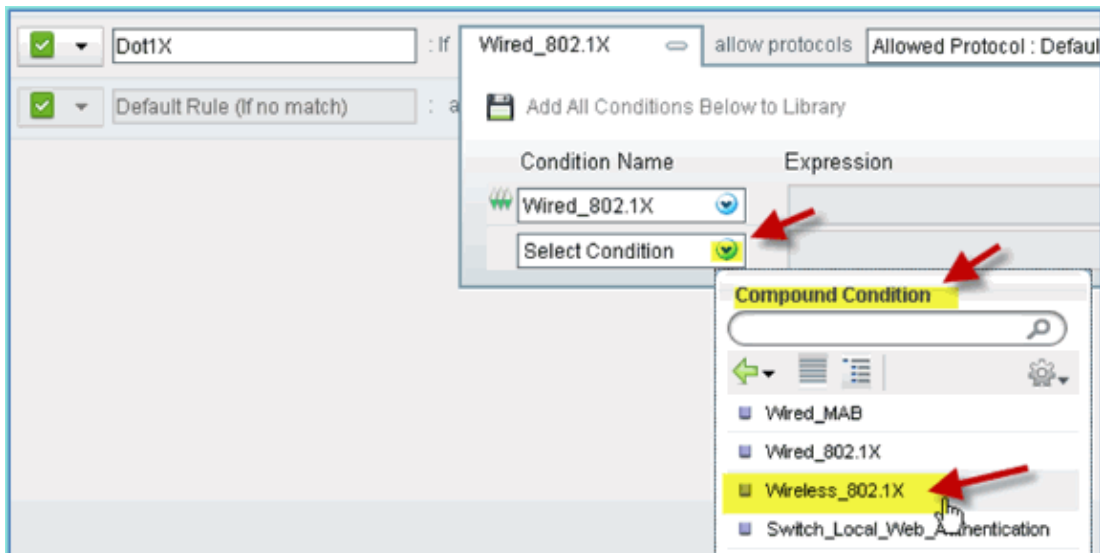
The ISE needs to be configured for authenticating 802.1x wireless clients and to use Active Directory as the identity store.

Complete these steps:

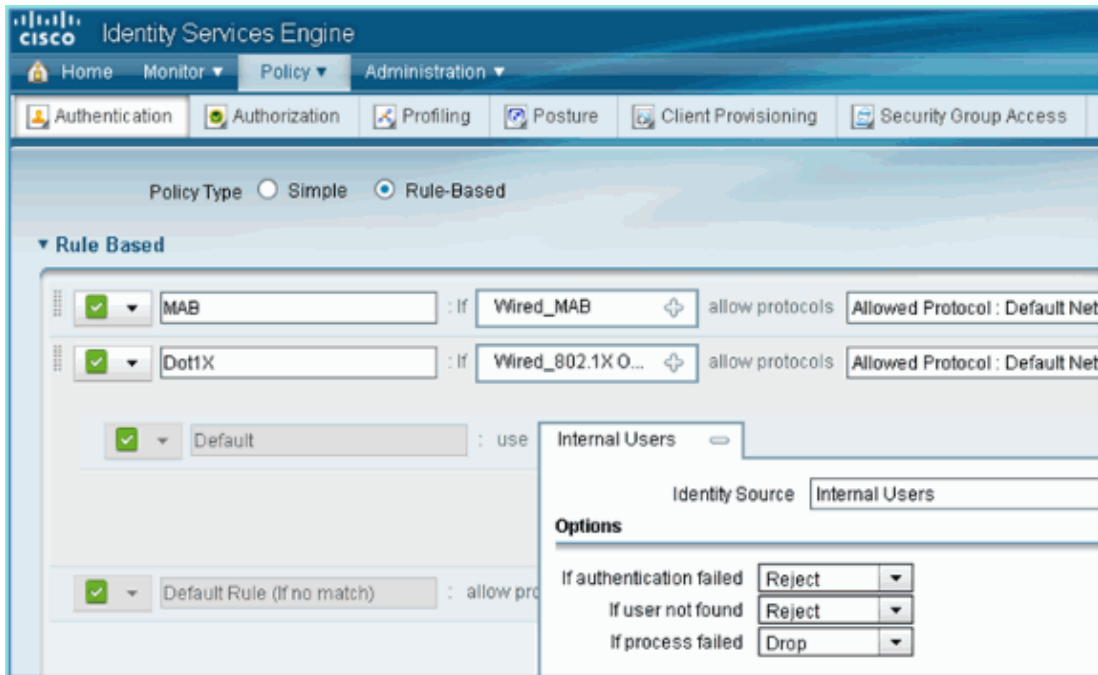
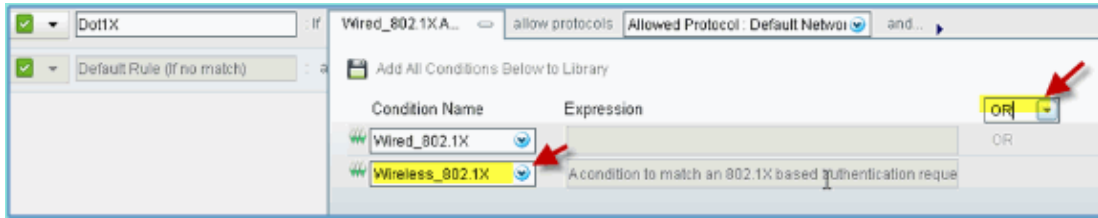
1. From ISE navigate to **Policy > Authentication**.
2. Click to expand the Dot1x > Wired_802.1X (-).
3. Click on the gear icon to **Add Condition from Library**.



4. From the condition selection drop-down, choose **Compound Condition > Wireless_802.1X**.



5. Set the Express condition to **OR**.
6. Expand the after allow protocols option, and accept the default Internal Users (default).



7. Leave everything else at default. Click **Save** to complete the steps.

Bootstrap Wireless LAN Controller

Connecting WLC to a Network

A Cisco 2500 Wireless LAN Controller deployment guide is also available at [Cisco 2500 Series Wireless Controller Deployment Guide](#).

Configure the Controller Using Startup Wizard

```
(Cisco Controller)
Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
ISE-Podx Enter Administrative User Name (24 characters max): admin
Enter Administrative Password
(3 to 24 characters): Cisco123
Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
```

```
Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: 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]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
Configure a NTP server now? [YES][no]: no
Configure the ntp system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
Configuration saved!
Resetting system with new configuration...
Restarting system.
```

Neighbor Switch Configuration

The controller is connected to the Ethernet port on the neighboring switch (Fast Ethernet 1). The neighbor switch port is configured as an 802.1Q trunk and allows all VLANs on the trunk. The native VLAN 10 allows the management interface of the WLC to be connected.

The 802.1Q switch port configuration is as follows:

```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

Add Authentication Servers (ISE) to WLC

The ISE needs to be added to the WLC in order to enable 802.1X and the CoA feature for wireless endpoints.

Complete these steps:

1. Open a browser, then connect to the pod WLC (using secure HTTP) > <https://wlc>.
2. Navigate to **Security > Authentication > New**.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

RADIUS Authentication Servers > New

Server Index (Priority) 1

Server IP Address 10.10.10.70

Shared Secret Format ASCII

Shared Secret *****

Confirm Shared Secret *****

Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number 1812

Server Status Enabled

Support for RFC 3576 Enabled

Server Timeout 2 seconds

Network User Enable

Management Enable

IPSec Enable

3. Enter these values:

- ◆ Server IP Address: 10.10.10.70 (check assignment)
- ◆ Shared Secret: cisco
- ◆ Support for RFC 3576 (CoA): Enabled (default)
- ◆ Everything else: Default

4. Click **Apply** to continue.

5. Select **RADIUS Accounting > add NEW**.

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT C

Security RADIUS Accounting Servers > New

AAA

- General
- RADIUS
 - Authentication
 - Accounting
 - Fallback
- TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies

Local EAP

Priority Order

Certificate

Server Index (Priority) 2

Server IP Address 10.10.10.70

Shared Secret Format ASCII

Shared Secret *****

Confirm Shared Secret *****

Port Number 1813

Server Status Enabled

Server Timeout 2 seconds

Network User Enable

IPSec Enable

6. Enter these values:

- ◆ Server IP Address: 10.10.10.70
- ◆ Shared Secret: cisco
- ◆ Everything else: Default

7. Click **Apply**, then save the Configuration for the WLC.

Create WLC Employee Dynamic Interface

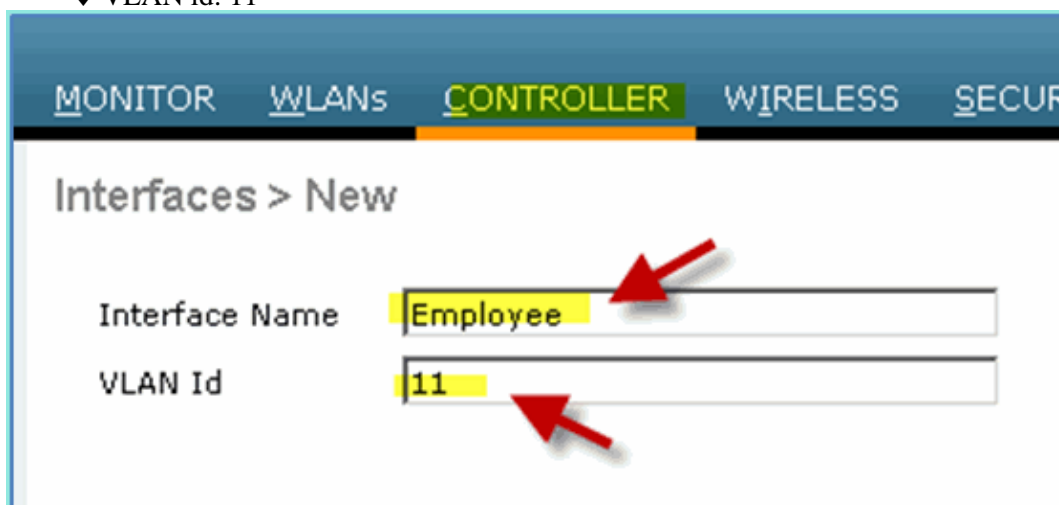
Complete these steps in order to add a new dynamic interface for the WLC and map it to the Employee VLAN:

1. From WLC, navigate to **Controller > Interfaces**. Then, click **New**.



2. From WLC, navigate to **Controller > Interfaces**. Enter the following:

- ◆ Interface Name: Employee
- ◆ VLAN id: 11



3. Enter the following for Employee interface:

- ◆ Port Number: 1
- ◆ VLAN Identifier: 11
- ◆ IP Address: 10.10.11.5
- ◆ Netmask: 255.255.255.0
- ◆ Gateway: 10.10.11.1
- ◆ DHCP: 10.10.10.10

Configuration

Quarantine

Quarantine Vlan Id

Physical Information

Port Number

Backup Port

Active Port

Enable Dynamic AP Management

Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

DHCP Information

Primary DHCP Server

Secondary DHCP Server

4. Confirm that the new employee dynamic interface is created.

CISCO

MONITOR | WLANs | **CONTROLLER** | WIRELESS | SECURITY | MANAGEMENT | COMM

Controller

General

Inventory

Interfaces

Interface Groups

Multicast

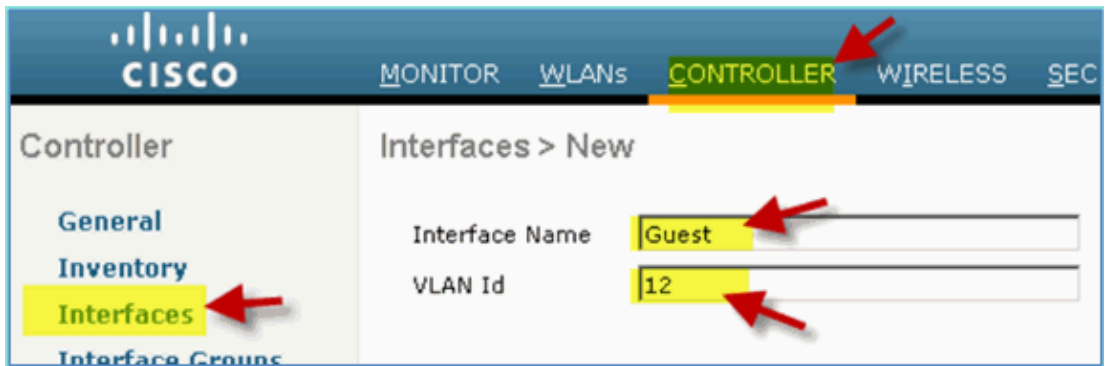
Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type
employee	11	10.10.11.5	Dynamic
management	untagged	10.10.10.5	Static
virtual	N/A	1.1.1.1	Static

Create WLC Guest Dynamic Interface

Complete these steps in order to add a new dynamic interface for the WLC and map it to the Guest VLAN:

1. From WLC, navigate to **Controller > Interfaces**. Then, click **New**.
2. From WLC, navigate to **Controller > Interfaces**. Enter the following:
 - ◆ Interface Name: Guest
 - ◆ VLAN id: 12



3. Enter these for Guest interface:

- ◆ Port Number: 1
- ◆ VLAN Identifier: 12
- ◆ IP Address: 10.10.12.5
- ◆ Netmask: 255.255.255.0
- ◆ Gateway: 10.10.12.1
- ◆ DHCP: 10.10.10.10

Configuration

Quarantine

Quarantine Vlan Id

Physical Information

Port Number

Backup Port

Active Port

Enable Dynamic AP Management

Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

DHCP Information

Primary DHCP Server

Secondary DHCP Server

Access Control List

ACL Name

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

4. Confirm that the guest interface has been added.

CISCO MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMAND

Controller

- General
- Inventory
- Interfaces**
- Interface Groups
- Multicast
- Internal DHCP Server

Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type
employee	11	10.10.11.5	Dynamic
guest	12	10.10.12.5	Dynamic
management	untagged	10.10.10.5	Static
virtual	N/A	1.1.1.1	Static

Add 802.1x WLAN

From the initial bootstrap of WLC, there might have been a default WLAN created. If so, modify it or create a new WLAN to support wireless 802.1X authentication as instructed in the guide.

Complete these steps:

1. From WLC, navigate to **WLAN > Create New**.



2. For the WLAN, enter the following:

- ◆ Profile Name: pod1x
- ◆ SSID: Same



3. For the WLAN settings > General tab, use the following:

- ◆ Radio Policy: All
- ◆ Interface/Group: management
- ◆ Everything else: default

MONITOR WLANS CONTROLLER WIRELESS SECURITY

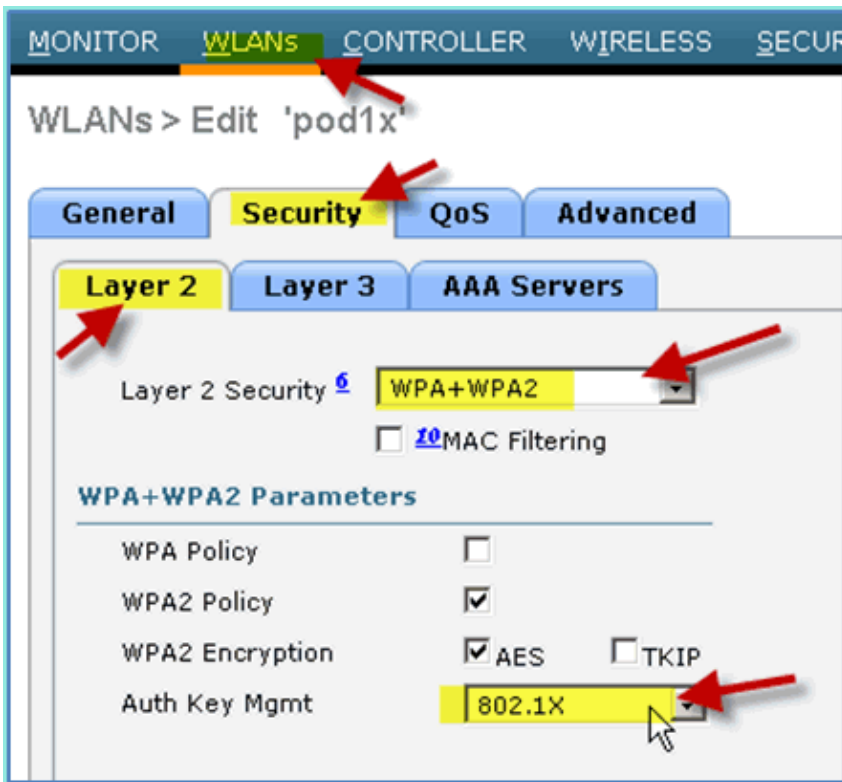
WLANs > Edit 'pod1x'

General Security QoS Advanced

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab w
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

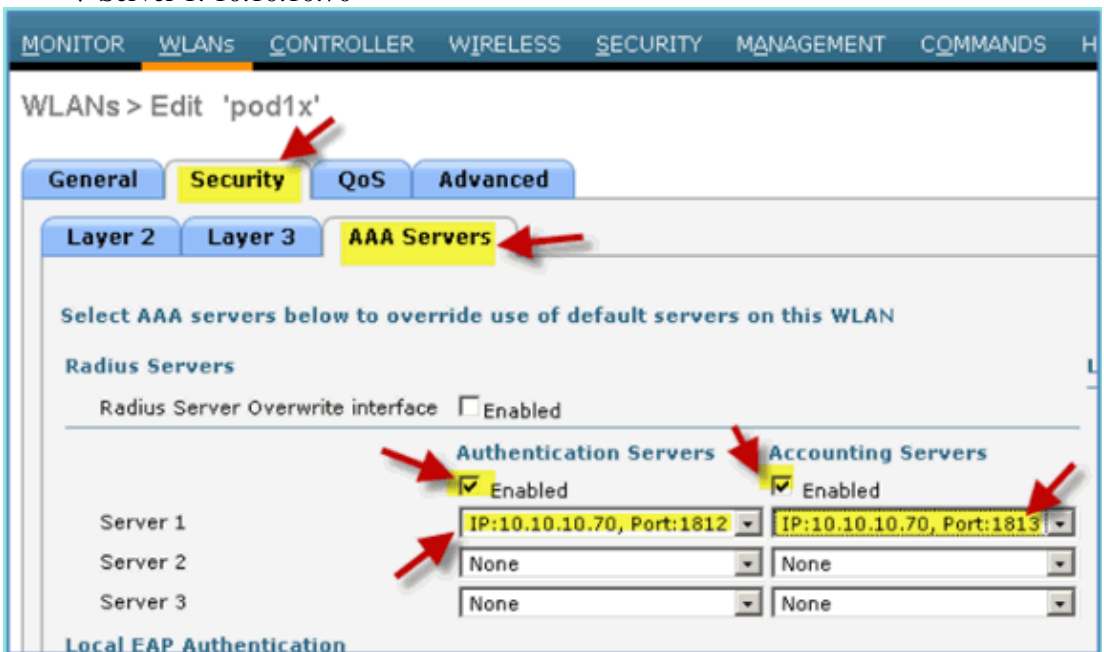
4. For the WLAN > Security tab > Layer 2, set the following:

- ◆ Layer 2 Security:WPA+WPA2
- ◆ WPA2 Policy / Encryption: Enabled / AES
- ◆ Auth Key Mgmt: 802.1X



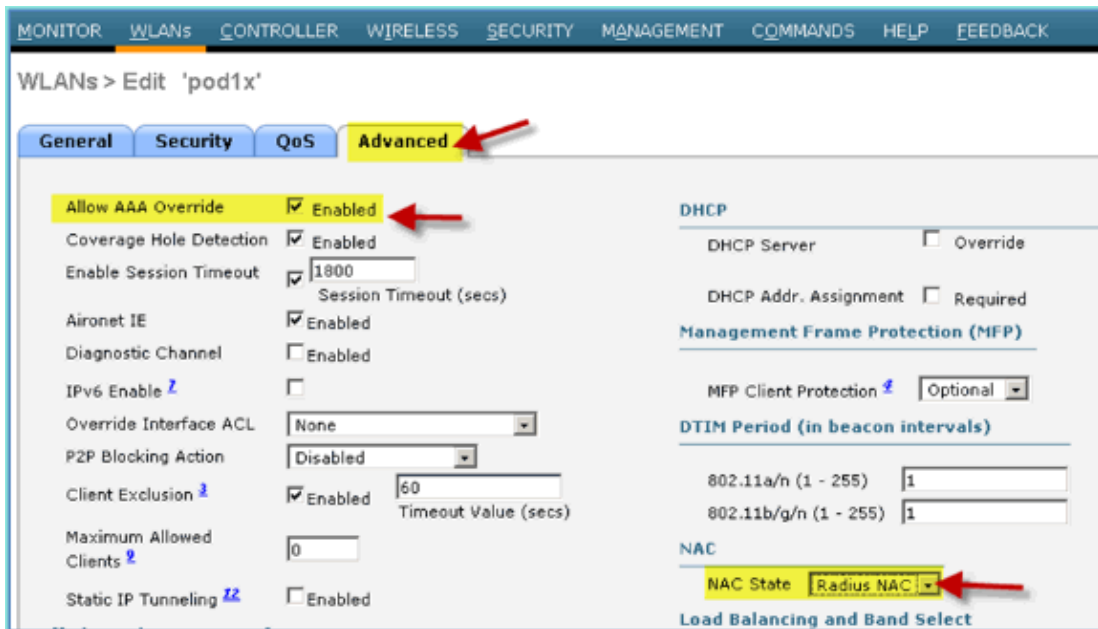
5. For the WLAN > Security tab > AAA Servers, set the following:

- ◆ Radio Server Overwrite Interface: Disabled
- ◆ Authentication/Accounting Servers: Enabled
- ◆ Server 1: 10.10.10.70

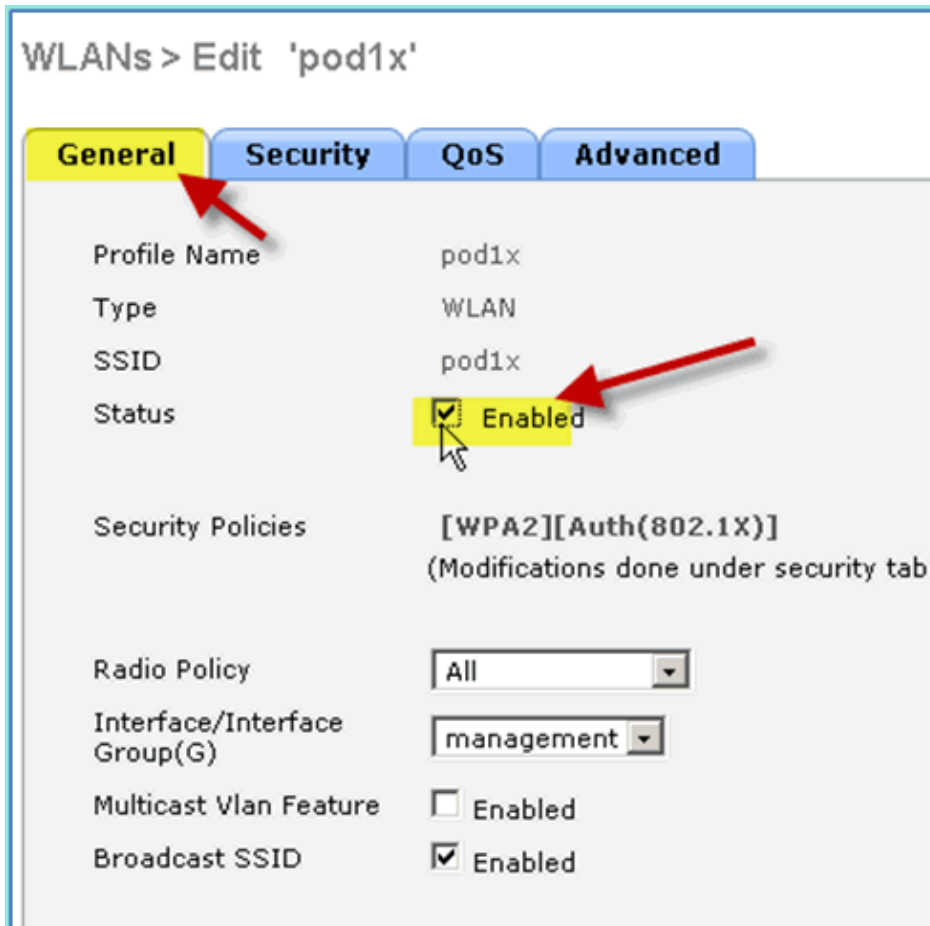


6. For the WLAN > Advanced tab, set the following:

- ◆ Allow AAA Override: Enabled
- ◆ NAC State: Radius NAC (selected)



7. Back to the WLAN > General tab > Enable WLAN (check box).



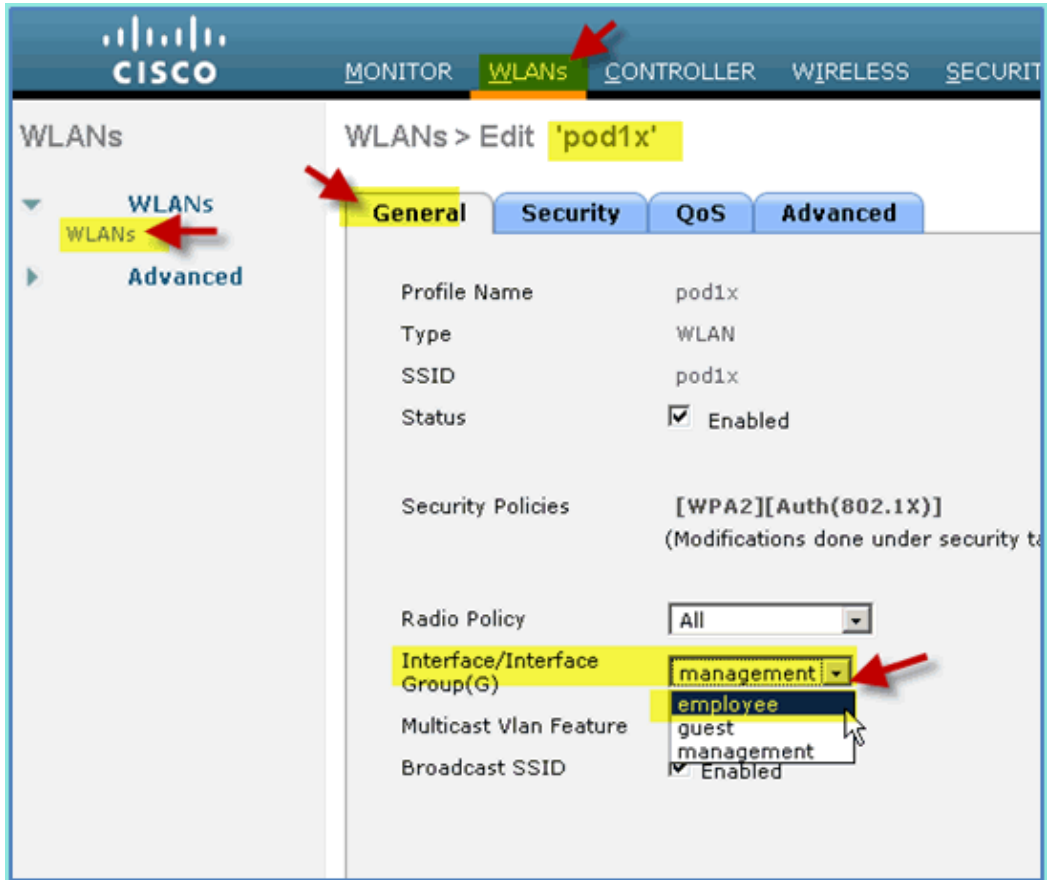
Test WLC Dynamic Interfaces

You need to make a quick check for valid employee and guest interfaces. Use any device to associate to the WLAN, then change the WLAN interface assignment.

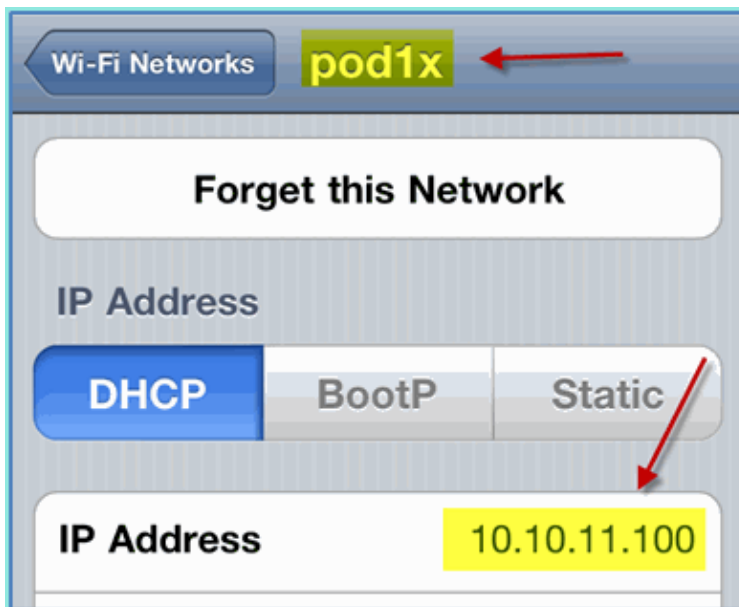
1. From WLC, navigate to **WLAN > WLANs**. Click to edit your secure SSID created in the earlier

exercise.

2. Change the Interface/Interface Group to **Employee**, then click **Apply**.



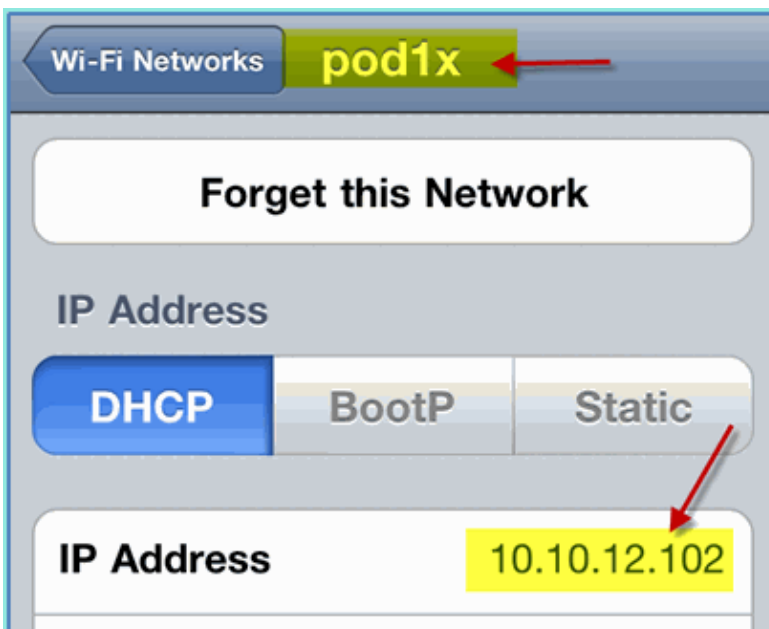
3. If configured properly, a device receives an IP address from the employee VLAN (10.10.11.0/24). This example shows an iOS device that gets a new IP address.



4. Once the previous interface has been confirmed, change the WLAN interface assignment to **Guest**, then click **Apply**.



5. If configured properly, a device receives an IP address from the guest VLAN (10.10.12.0/24). This example shows an iOS device that gets a new IP address.



6. **IMPORTANT:** Change the Interface assignment back to the original management.
 7. Click **Apply** and save the Configuration for the WLC.

Wireless Authentication for iOS (iPhone/iPad)

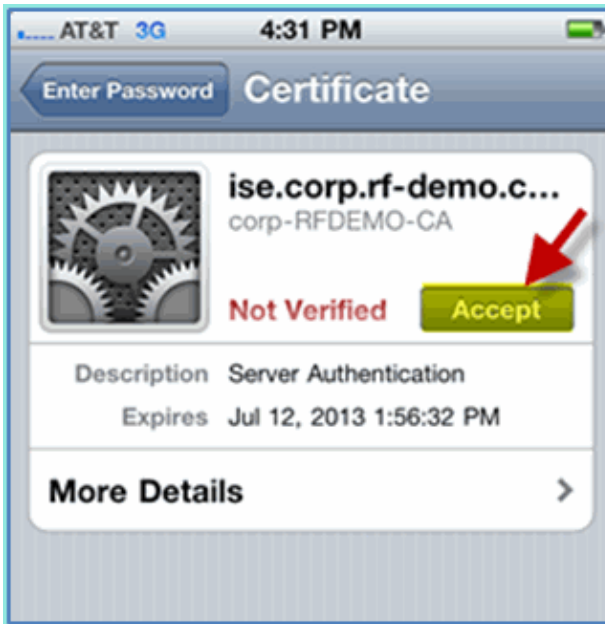
Associate to the WLC via an authenticated SSID an INTERNAL user (or integrated, AD User) using an iOS device such as an iPhone, iPad, or iPod. Skip these steps if not applicable.

1. On the iOS device, go to the WLAN settings. Enable WIFI, then select the 802.1X enabled SSID created in the previous section.
2. Provide this information in order to connect:

- ◆ Username: employee (internal Employee) or contractor (internal Contractor)
- ◆ Password: XXXX



3. Click to accept the ISE certificate.



4. Confirm that the iOS device is getting an IP address from the management (VLAN10) interface.



5. On the WLC > Monitor > Clients, verify the endpoint information including use, state, and EAP type.

The screenshot shows the Cisco ISE Monitor interface. The left sidebar contains navigation options: Monitor, Summary, Access Points, Cisco CleanAir, Statistics, CDP, Rogues, Clients, and Multicast. The main content area is titled 'Clients > Detail' and is divided into two sections: 'Client Properties' and 'Security Information'.

Client Properties:

- MAC Address: 5c:59:48:40:82:8d
- IP Address: 10.10.10.102
- Client Type: Regular
- User Name: aduser
- Port Number: 1
- Interface: management
- Mobility Peer IP Address: N/A
- Policy Manager State: RUN
- Management Frame Protection: No

Security Information:

- Security Policy Completed: Yes
- Policy Type: RSN (WPA2)
- Encryption Cipher: CCMP (AES)
- EAP Type: PEAP
- SNMP NAC State: Access
- Radius NAC State: RUN
- AAA Override ACL Name: none

6. Similarly, the client information can be provided by ISE > Monitor > Authentication page.

The screenshot shows the Cisco ISE Identity Services Engine Authentication page. The top navigation bar includes Home, Monitor, Policy, and Administration. Below the navigation bar are tabs for Authentications, Alarms, Reports, and Troubleshoot. The main content area features a table with columns for Time, Status, Details, Username, Endpoint ID, Network Device, Authorization Profiles, and Ident.

Time	Status	Details	Username	Endpoint ID	Network Device	Authorization Profiles	Ident
Jul 13, 11 04:39:36.573 PM	✓		aduser	5C-59-48-40-82-8D	WLC	PermitAccess	
Jul 13, 11 04:38:46.285 PM	✓		aduser	5C-59-48-40-82-8D	WLC	PermitAccess	

A red arrow points to the 'Details' icon in the first row of the table.

7. Click the **Details** icon in order to drill down to the session for in-depth information of the session.

CISCO Identity Services Engine

Showing Page 1 of 1 | First Prev

AAA Protocol > RADIUS Authentication Detail

RADIUS Audit Session ID : 0a0a0a050000000d4e1e2a45
 AAA session ID : ise/99967658/11
 Date : July 13,2011

Generated on July 13, 2011 4:41:11 PM PDT

Authentication Summary	
Logged At:	July 13,2011 4:39:36.573 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	<u>aduser</u>
MAC/IP Address:	<u>5C:59:48:40:82:8D</u>
Network Device:	<u>WLC : 10.10.10.5 :</u>
Allowed Protocol:	<u>Default Network Access</u>
Identity Store:	AD1
Authorization Profiles:	PermitAccess
SGA Security Group:	
Authentication Protocol :	PEAP(EAP-MSCHAPv2)

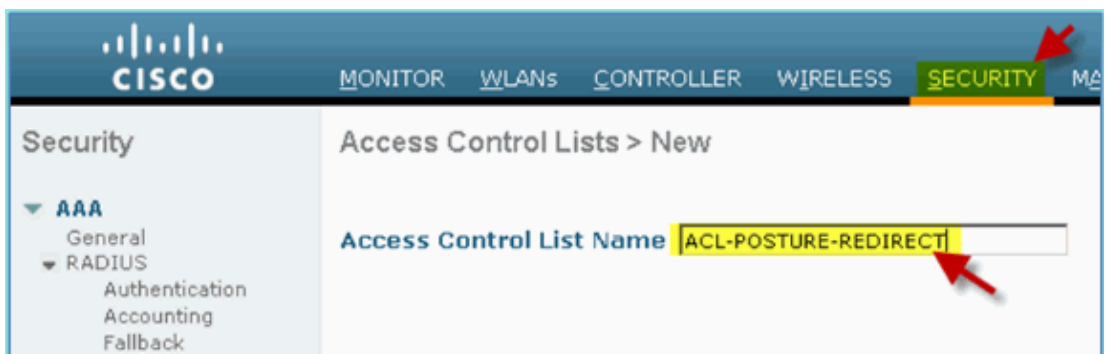
Add Posture Redirect ACL to WLC

Posture redirect ACL is configured on the WLC, where ISE will use to restrict client for posture. Effectively and at a minimum the ACL permits traffic between ISE. Optional rules can be added in this ACL if needed.

1. Navigate to **WLC > Security > Access Control Lists > Access Control Lists**. Click **New**.



2. Provide a name (ACL-POSTURE-REDIRECT) for the ACL.



3. Click **Add New Rule** for the new ACL. Set the following values to ACL sequence #1. Click **Apply** when finished.

- ◆ Source: Any
- ◆ Destination: IP Address 10.10.10.70, 255.255.255.255
- ◆ Protocol: Any
- ◆ Action: Permit

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Access Control Lists > Rules > Edit

Sequence:

Source:

Destination: IP Address: Netmask:

Protocol:

DSCP:

Direction:

Action:

4. Confirm sequence has been added.

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 /	10.10.10.70 /	Any	Any	Any	Any	Any	0

5. Click **Add New Rule**. Set the following values to ACL sequence #2. Click **Apply** when finished.

- ◆ Source: IP Address 10.10.10.70, 255.255.255.255
- ◆ Destination: Any
- ◆ Protocol: Any
- ◆ Action: Permit

Sequence:

Source: IP Address: Netmask:

Destination:

Protocol:

DSCP:

Direction:

Action:

6. Confirm sequence has been added.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
<u>1</u>	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
<u>2</u>	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any

7. Set the following values to ACL sequence #3. Click **Apply** when finished.

- ◆ Source: Any

- ◆ Destination: Any
- ◆ Protocol: UDP
- ◆ Source Port: DNS
- ◆ Destination Port: Any
- ◆ Action: Permit

The screenshot shows a configuration window for an ACL rule. The fields are as follows:

- Sequence: 3
- Source: Any
- Destination: Any
- Protocol: UDP
- Source Port: DNS
- Destination Port: Any
- DSCP: Any
- Direction: Any
- Action: Permit

8. Confirm sequence has been added.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
		0.0.0.0 /	255.255.255.255 /					
2	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
		255.255.255.255 /	0.0.0.0 /					
3	Permit	0.0.0.0 /	0.0.0.0 /	UDP	DNS	Any	Any	Any
		0.0.0.0 /	0.0.0.0 /					

9. Click **Add New Rule**. Set the following values to ACL sequence #4. Click **Apply** when finished.

- ◆ Source: Any
- ◆ Destination: Any
- ◆ Protocol: UDP
- ◆ Source Port: Any
- ◆ Destination Port: DNS
- ◆ Action: Permit

Sequence: 4

Source: Any

Destination: Any

Protocol: UDP

Source Port: Any

Destination Port: DNS

DSCP: Any

Direction: Any

Action: Permit

10. Confirm sequence has been added.

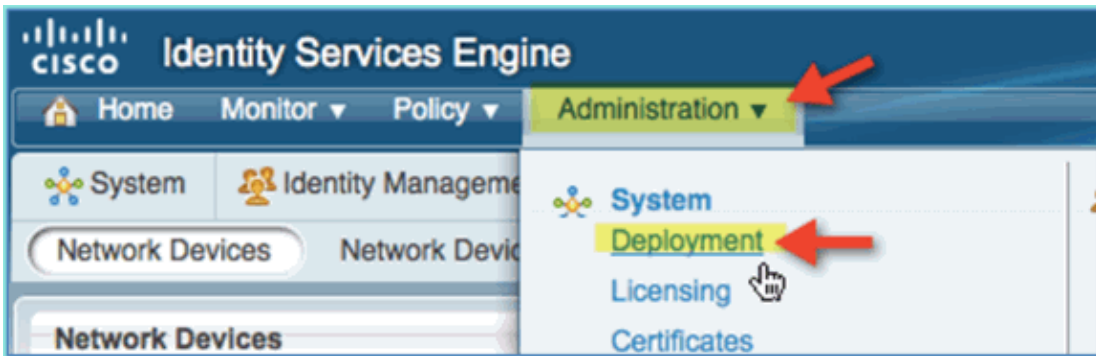
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
		0.0.0.0 /	255.255.255.255 /					
2	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
		255.255.255.255 /	0.0.0.0 /					
3	Permit	0.0.0.0 /	0.0.0.0 /	UDP	DNS	Any	Any	Any
		0.0.0.0 /	0.0.0.0 /					
4	Permit	0.0.0.0 /	0.0.0.0 /	UDP	Any	DNS	Any	Any
		0.0.0.0 /	0.0.0.0 /					

11. Save the current WLC configuration.

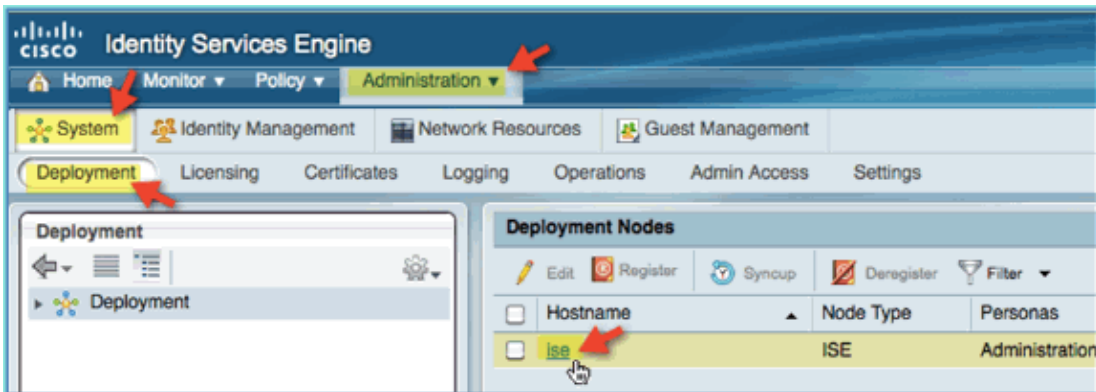
Enable Profiling Probes on ISE

The ISE needs to be configured as probes to effectively profile endpoints. By default, these options are disabled. This section shows how to configure ISE to be probes.

1. From ISE management, navigate to **Administration > System > Deployment**.

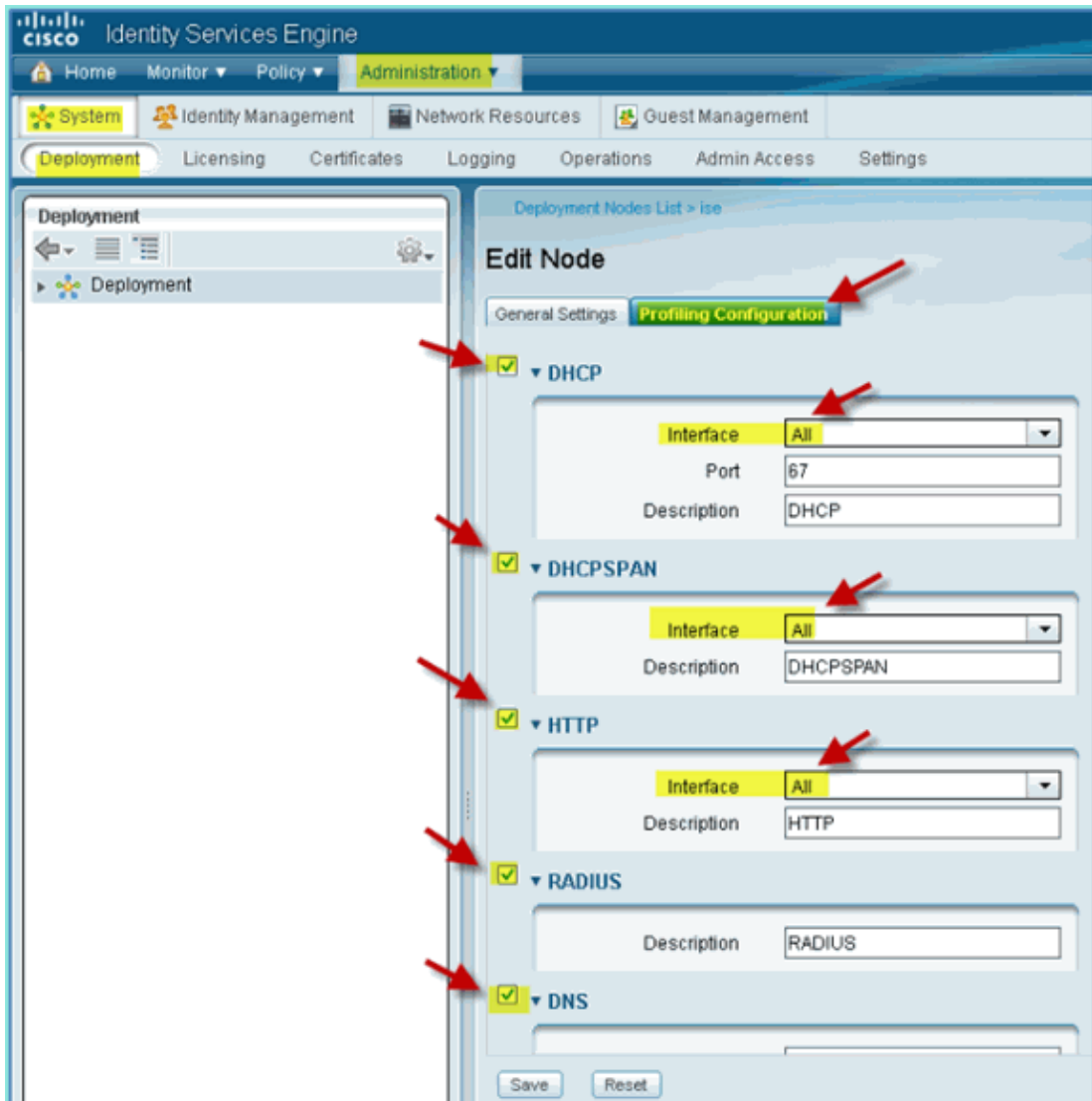


2. Choose ISE. Click **Edit ISE host**.



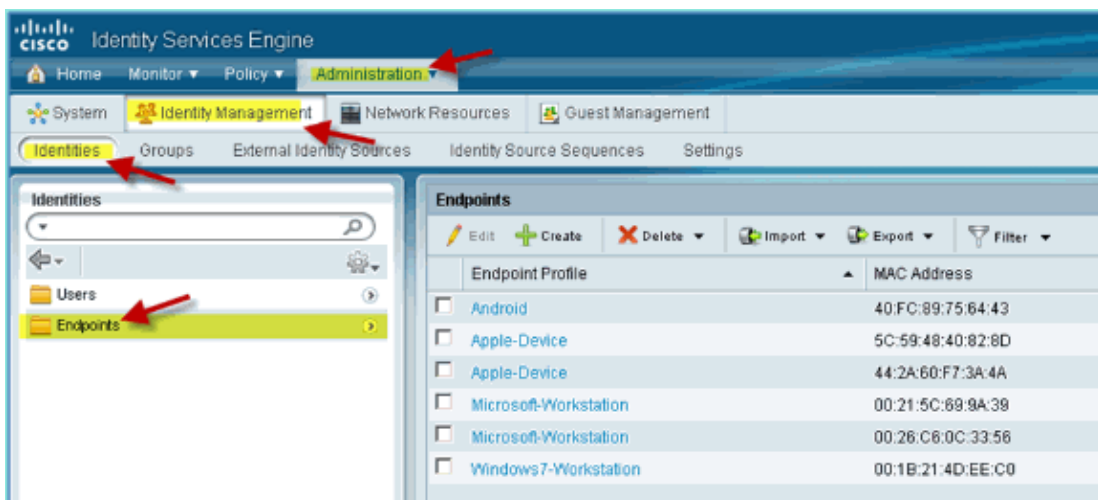
3. From the Edit Node page, select the Profiling Configuration and configure the following:

- ◆ DHCP: Enabled, All (or default)
- ◆ DHCPSPAN: Enabled, All (or default)
- ◆ HTTP: Enabled, All (or default)
- ◆ RADIUS: Enabled, N/A
- ◆ DNS: Enabled, N/A



4. Re-associate the devices (iPhone/iPads/Droids/Mac, etc.).
5. Confirm ISE endpoint identities. Navigate to **Administration > Identity Management > Identities**. Click on Endpoints to list what has been profiled.

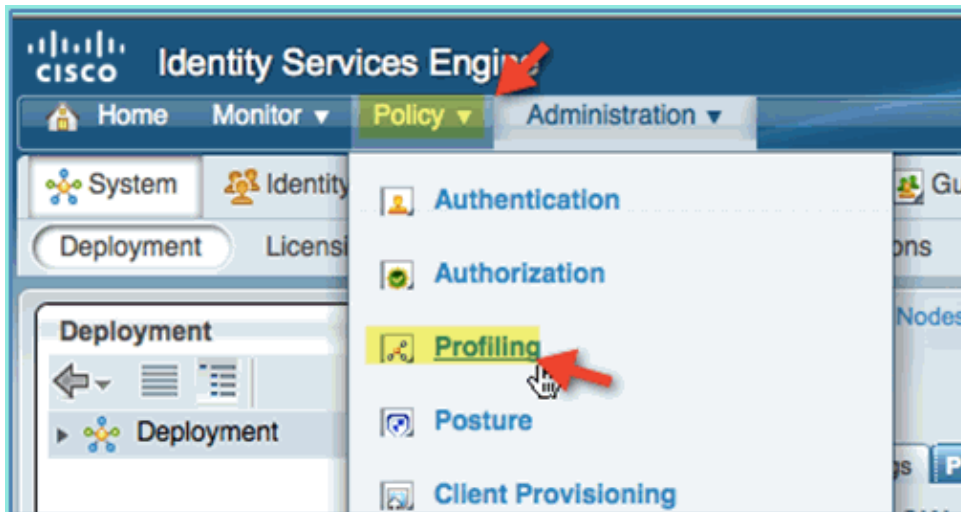
Note: The initial profiling is from RADIUS probes.



Enable ISE Profile Policies for Devices

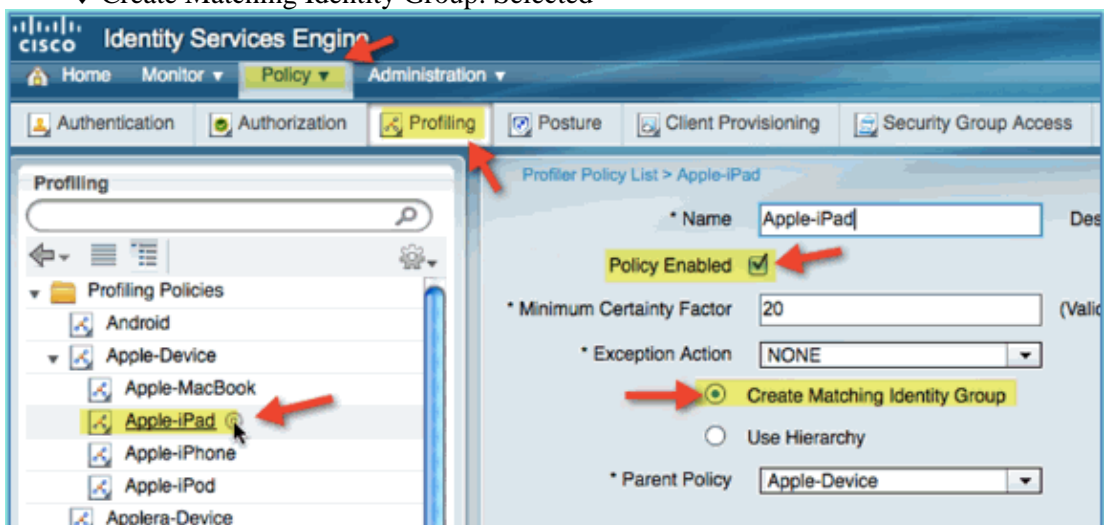
Out of the box, ISE provides a library of various endpoint profiles. Complete these steps in order to enable profiles for devices:

1. From ISE, navigate to **Policy > Profiling**.



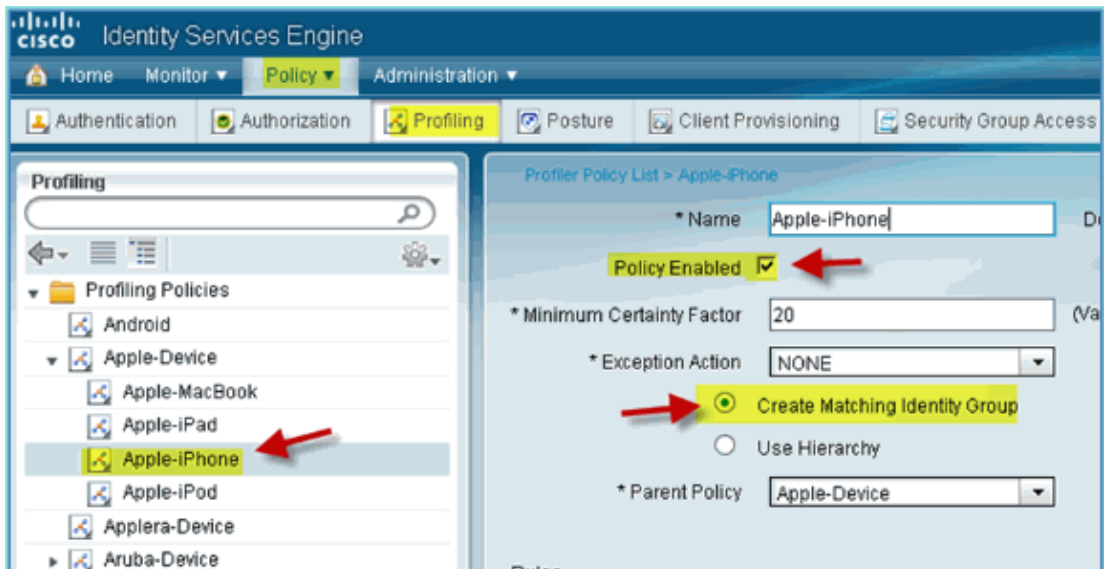
2. From the left pane, expand **Profiling Policies**.
3. Click **Apple Device > Apple iPad**, and set the following:

- ◆ Policy Enabled: Enabled
- ◆ Create Matching Identity Group: Selected



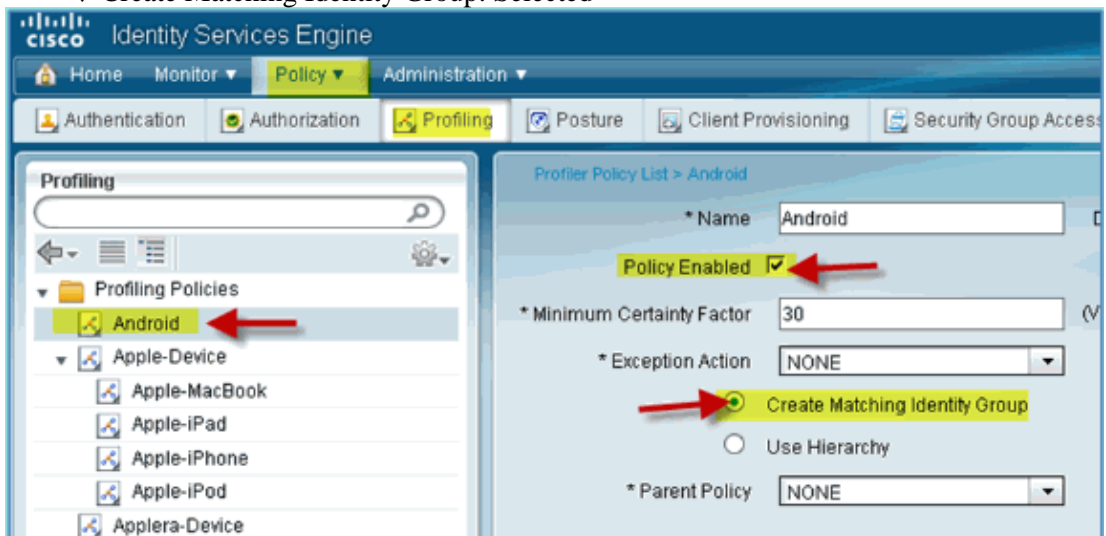
4. Click **Apple Device > Apple iPhone**, set the following:

- ◆ Policy Enabled: Enabled
- ◆ Create Matching Identity Group: Selected



5. Click **Android**, set the following:

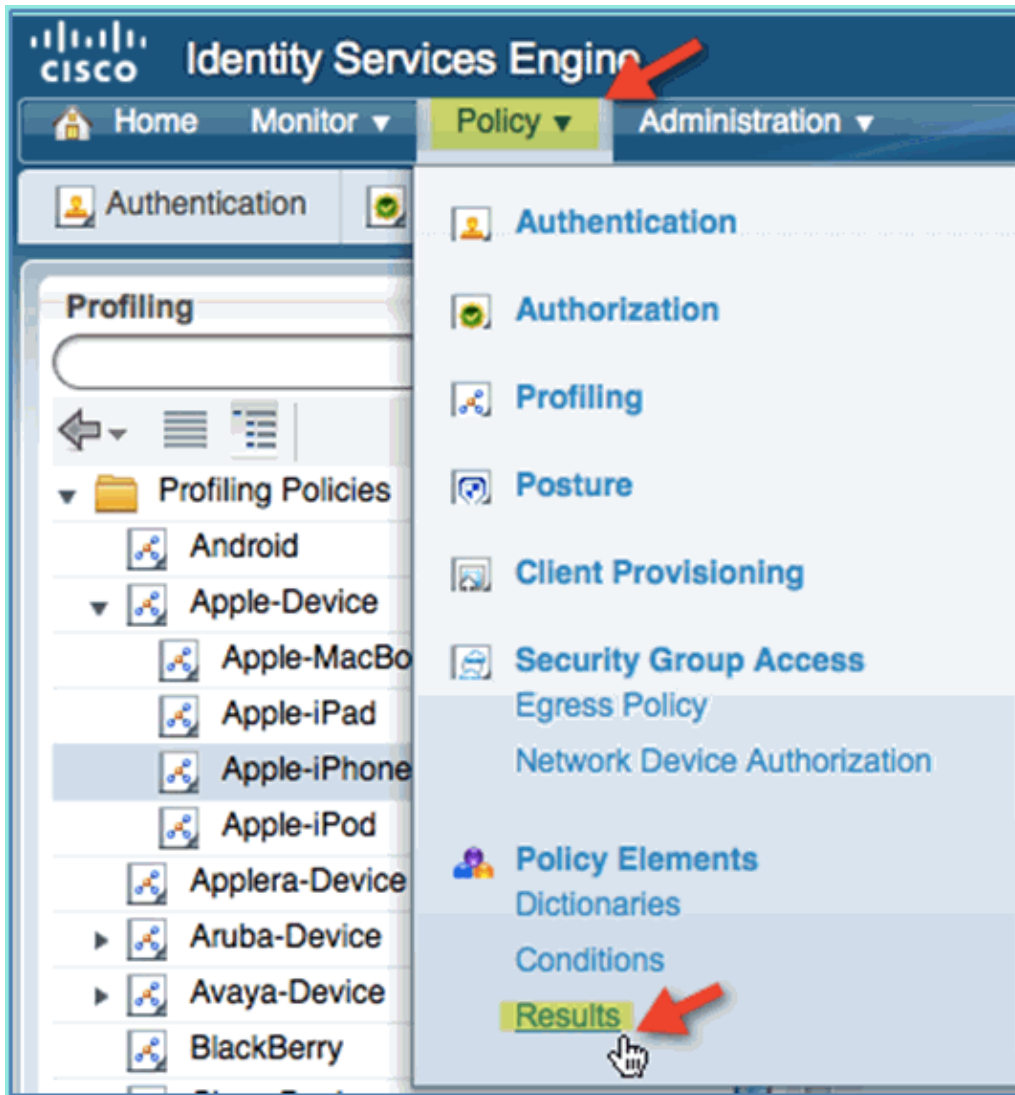
- ◆ Policy Enabled: Enabled
- ◆ Create Matching Identity Group: Selected



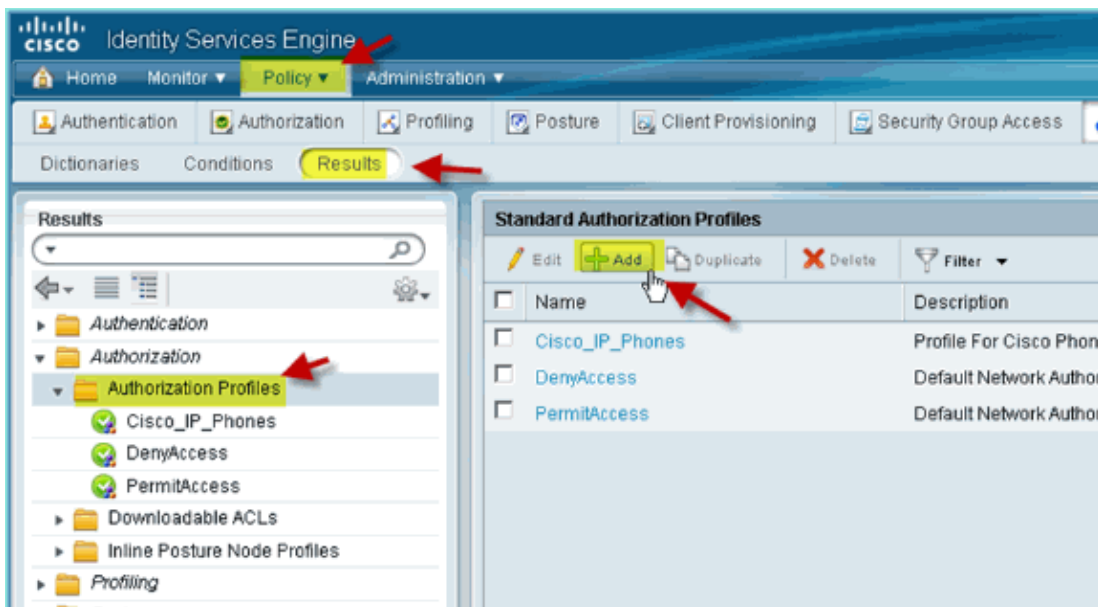
ISE Authorization Profile for Posture Discovery Redirect

Complete these steps in order to configure an authorization policy posture redirect allows new devices to be redirected to ISE for proper discovery and profiling:

1. From ISE, navigate to **Policy > Policy Elements > Results**.



2. Expand **Authorization**. Click **Authorization Profiles** (left pane) and click **Add**.



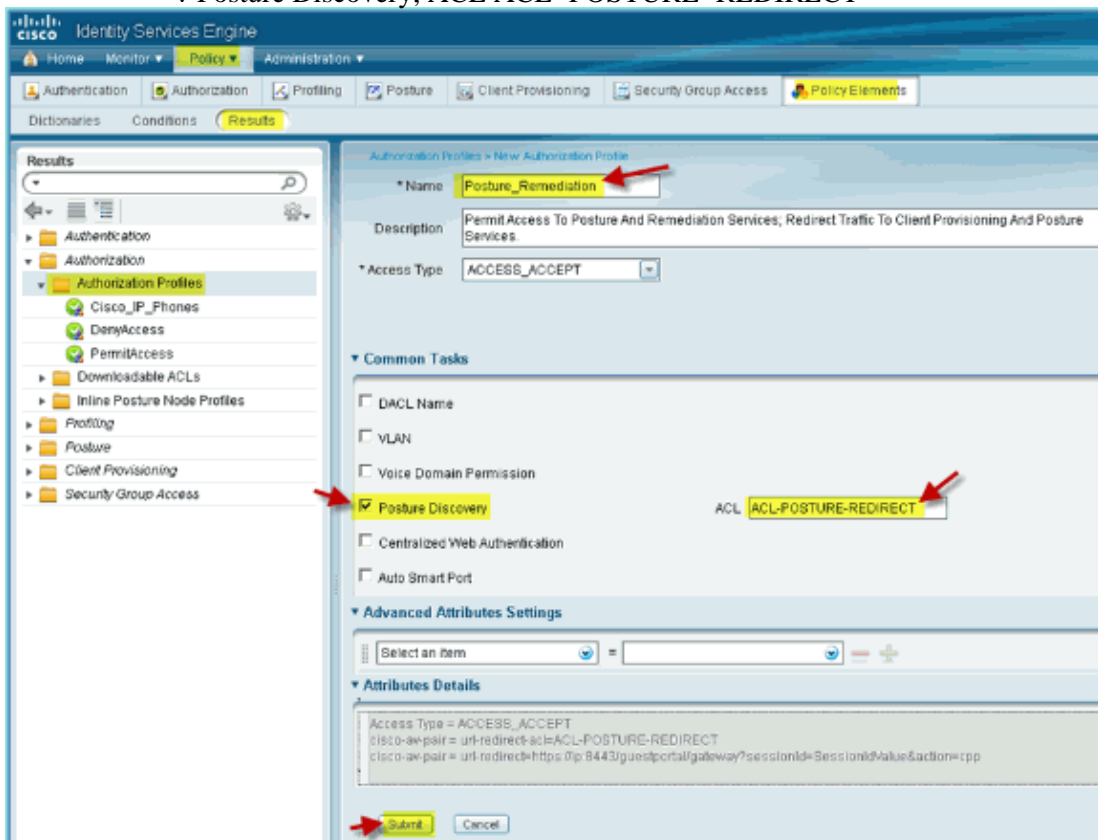
3. Create the authorization profile with the following:

- ◆ Name: Posture_Remediation
- ◆ Access Type: Access_Accept

◆ Common Tools:

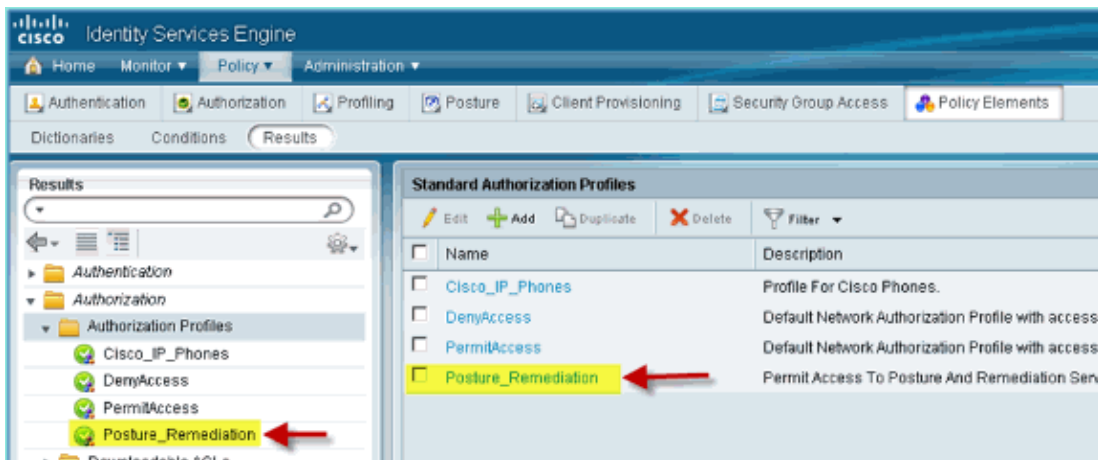
◇ Posture Discovery, Enabled

◇ Posture Discovery, ACL ACL-POSTURE-REDIRECT



4. Click **Submit** to complete this task.

5. Confirm that the new Authorization Profile is added.

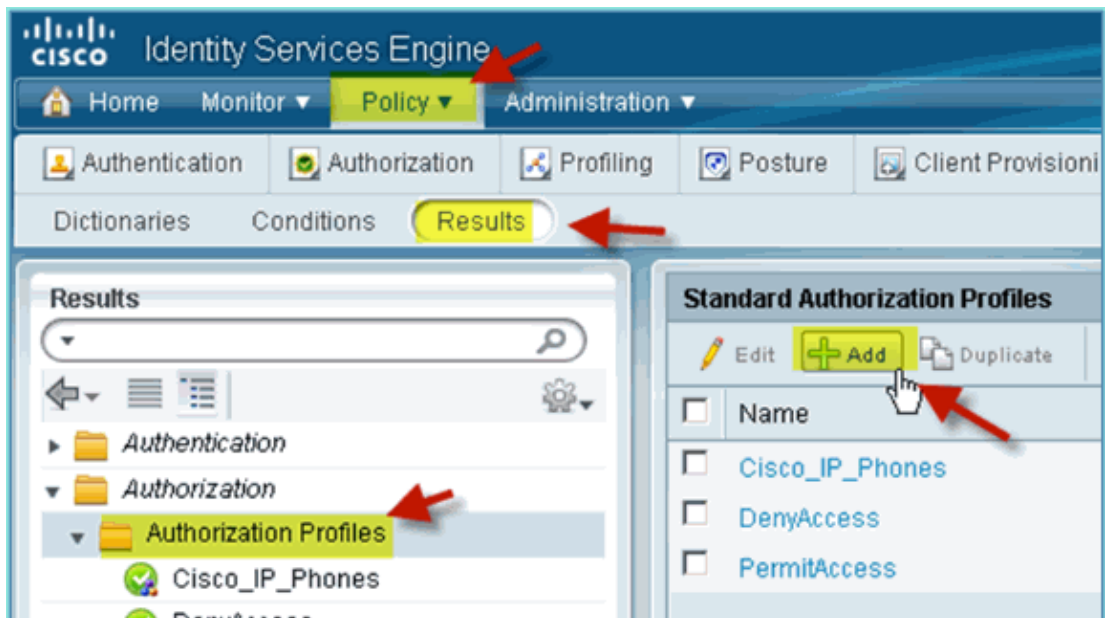


Create ISE Authorization Profile for Employee

Adding an authorization profile for an employee allows ISE to authorize and permit access with the assigned attributes. Employee VLAN 11 is assigned in this case.

Complete these steps:

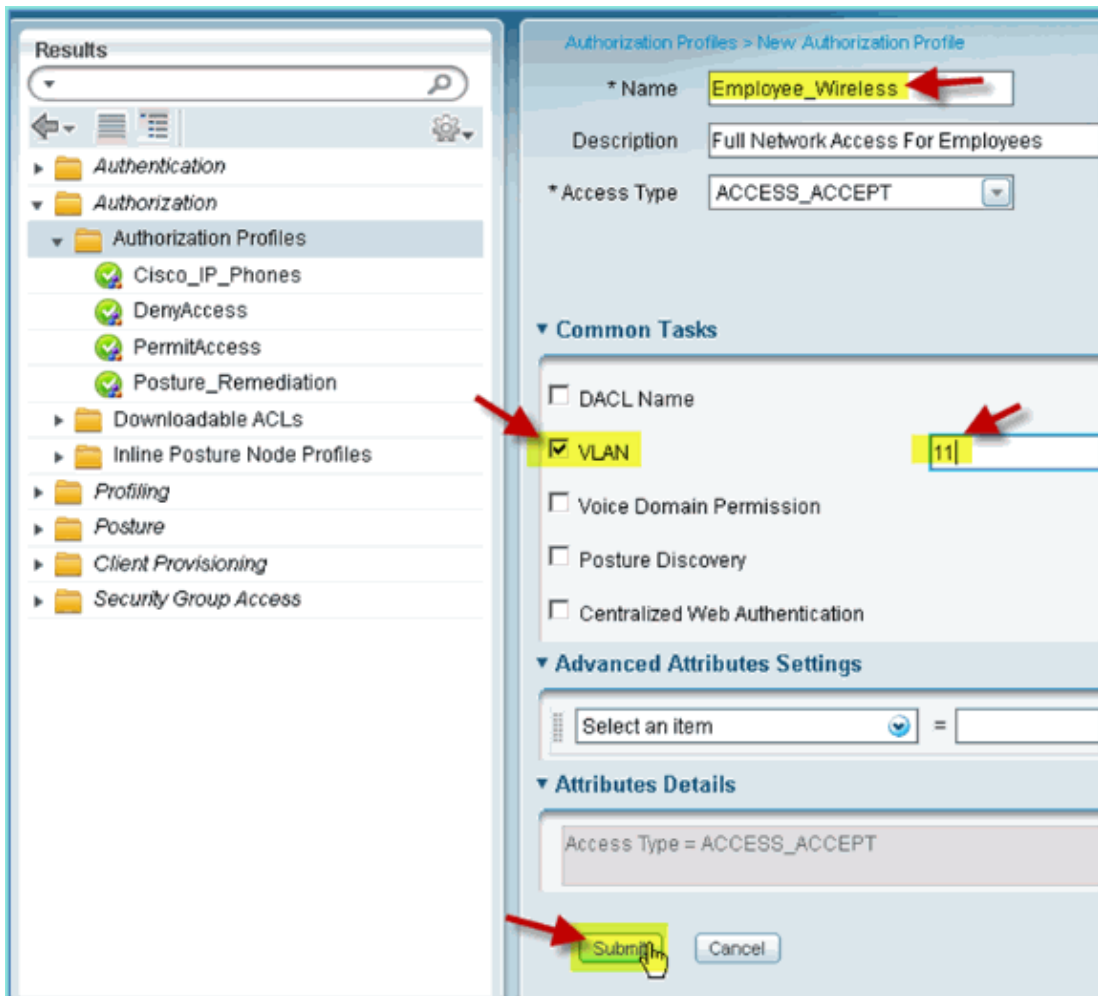
1. From ISE, navigate to **Policy > Results**. Expand **Authorization**, then click **Authorization Profiles** and click **Add**.



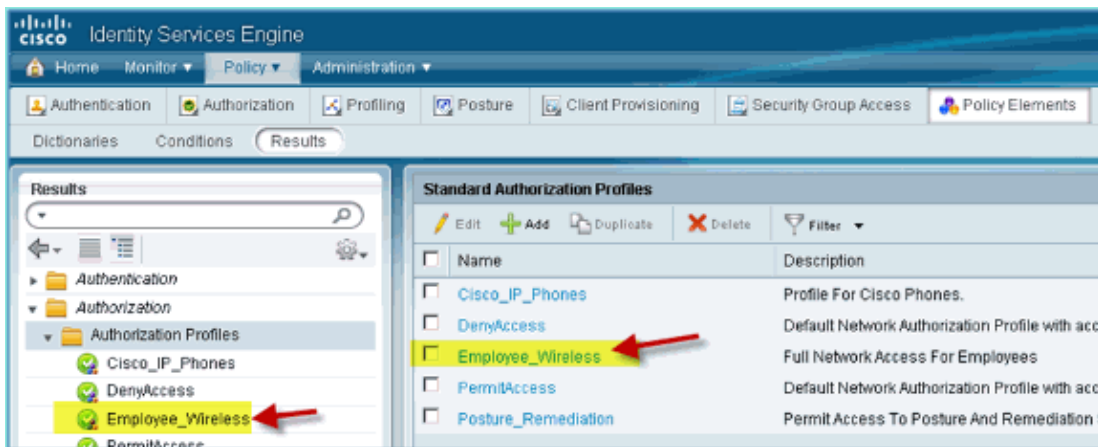
2. Enter the following for Employee authorization profile:

- ◆ Name: Employee_Wireless
- ◆ Common Tasks:
 - ◇ VLAN, Enabled
 - ◇ VLAN, sub value 11

3. Click **Submit** to complete this task.



4. Confirm that the new employee authorization profile was created.



Create ISE Authorization Profile for Contractor

Adding an authorization profile for a contractor allows ISE to authorize and permit access with the assigned attributes. Contractor VLAN 12 is assigned in this case.

Complete these steps:

1. From ISE, navigate to **Policy > Results**. Expand **Authorization**, then click **Authorization Profiles** and click **Add**.
2. Enter the following for Employee authorization profile:

◆ Name: Employee_Wireless

◆ Common Tasks:

◇ VLAN, Enabled

◇ VLAN, sub value 12

Authorization Profiles > New Authorization Profile

* Name: Contractor_Wireless

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks:

- DACL Name
- VLAN: 12
- Voice Domain Permission
- Posture Discovery
- Centralized Web Authentication
- Auto Smart Port

3. Click **Submit** to complete this task.

4. Confirm that the Contractor authorization profile was created.

Standard Authorization Profiles

Edit Add Duplicate Delete

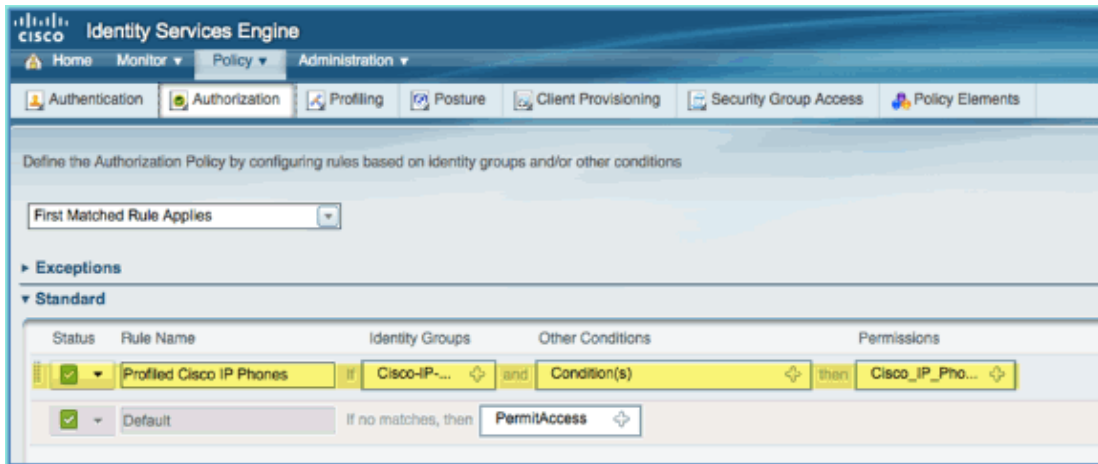
<input type="checkbox"/>	Name
<input type="checkbox"/>	Cisco_IP_Phones
<input checked="" type="checkbox"/>	Contractor_Wireless
<input type="checkbox"/>	DenyAccess
<input type="checkbox"/>	Employee_Wireless
<input type="checkbox"/>	PermitAccess
<input type="checkbox"/>	Posture_Remediation

Authorization Policy for Device Posture/Profiling

Little information is known about a new device when it first comes onto the network, an administrator will create the appropriate policy to allow unknown endpoints to be identified before permitting access. In this exercise, the authorization policy will be created so that a new device will be redirected to ISE for posture assessment (for mobile devices are agentless, therefore only profiling is relevant); endpoints will be redirected to the ISE captive portal and identified.

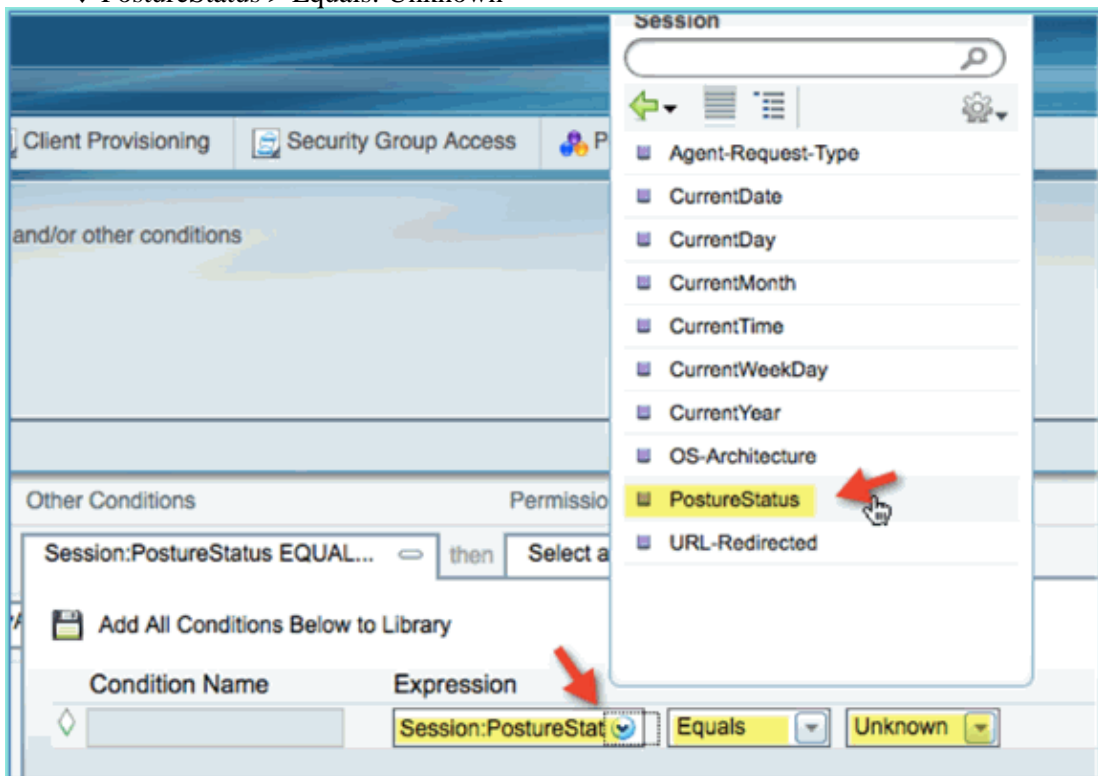
Complete these steps:

1. From ISE, navigate to **Policy > Authorization**.



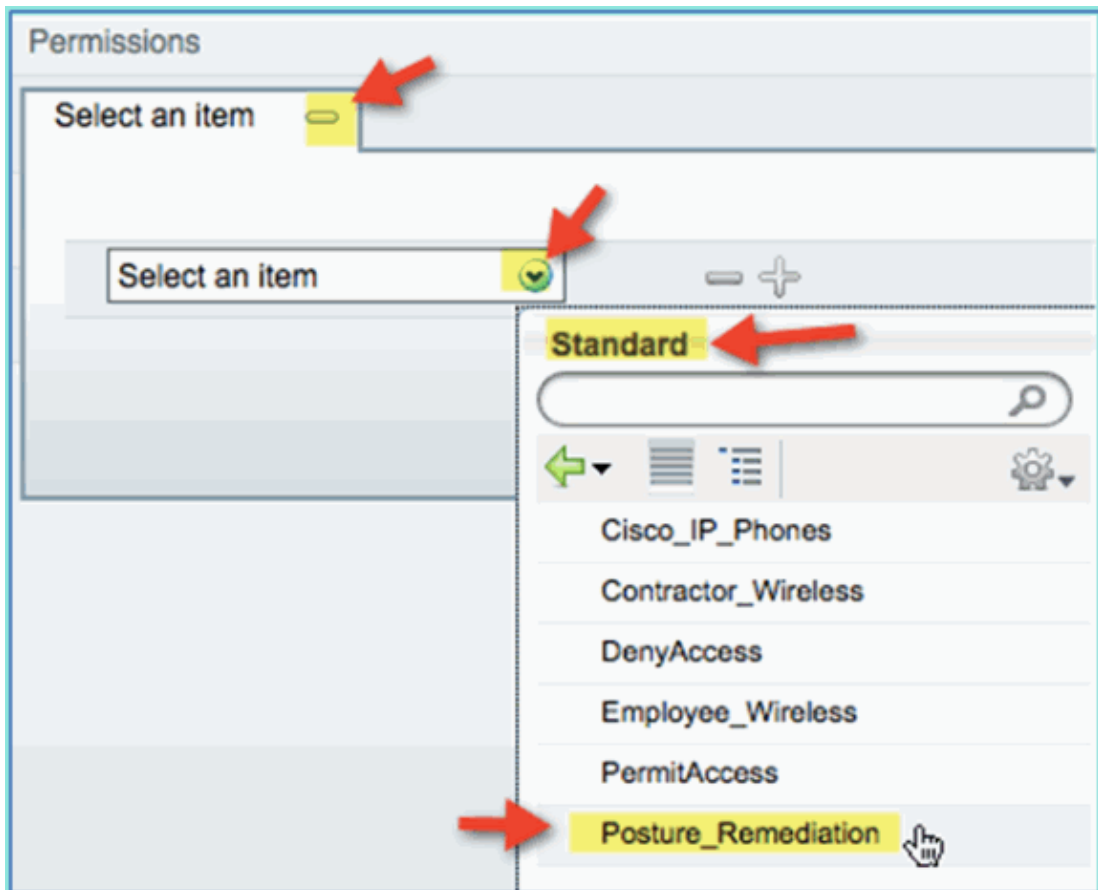
2. There is a policy for Profiled Cisco IP Phones. This is out of the box. Edit this as a posture policy.
3. Enter the following values for this policy:

- ◆ Rule Name: Posture_Remediation
- ◆ Identity Groups: Any
- ◆ Other Conditions > Create New: (Advanced) Session > PostureStatus
- ◆ PostureStatus > Equals: Unknown



4. Set the following for permissions:

- ◆ Permissions > Standard: Posture_Remediation



5. Click **Save**.

Note: Alternatively custom policy elements can be created to add ease of use.

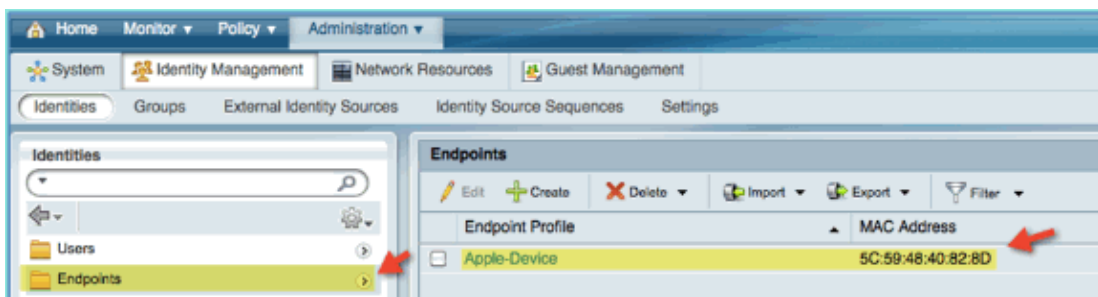
Testing Posture Remediation Policy

To simple demonstration can be performed to show that ISE is properly profiling a new device based on the posture policy.

1. From ISE, navigate to **Administration > Identity Management > Identities**.



2. Click **Endpoints**. Associate and connect a device (an iPhone in this example).

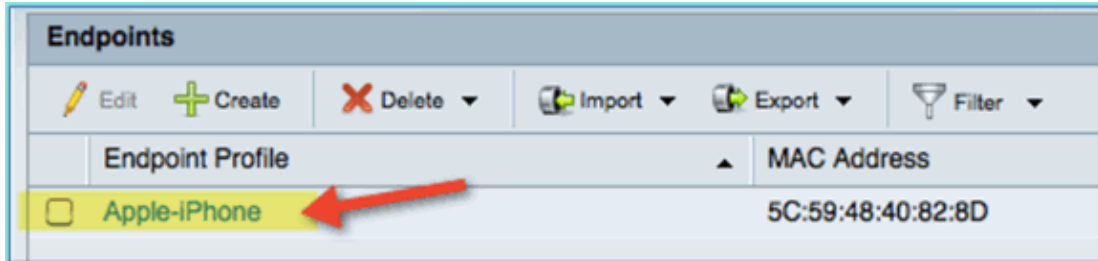


3. Refresh the Endpoints list. Observe what information is given.
4. From the endpoint device, browse to:

- ◆ URL: http://www (or 10.10.10.10)

The device is redirected. Accept any prompt for certificates.

5. After the mobile device has completely redirected, from ISE refresh the Endpoints list again. Observe what has changed. The previous endpoint (for example, Apple-Device) should have changed to Apple-iPhone etc. The reason is that the HTTP probe effectively obtains user-agent information, as part of the process of being redirected to the captive portal.

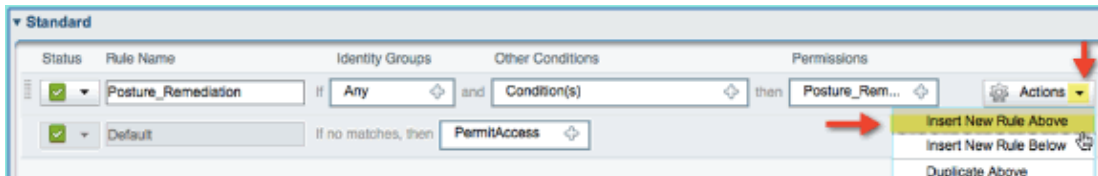


Authorization Policy for Differentiated Access

After successfully testing the posture authorization, continue to build policies to support differentiated access for the Employee and Contractor with known devices and different VLAN assignment specific to the user role (in this scenario, Employee and Contractor).

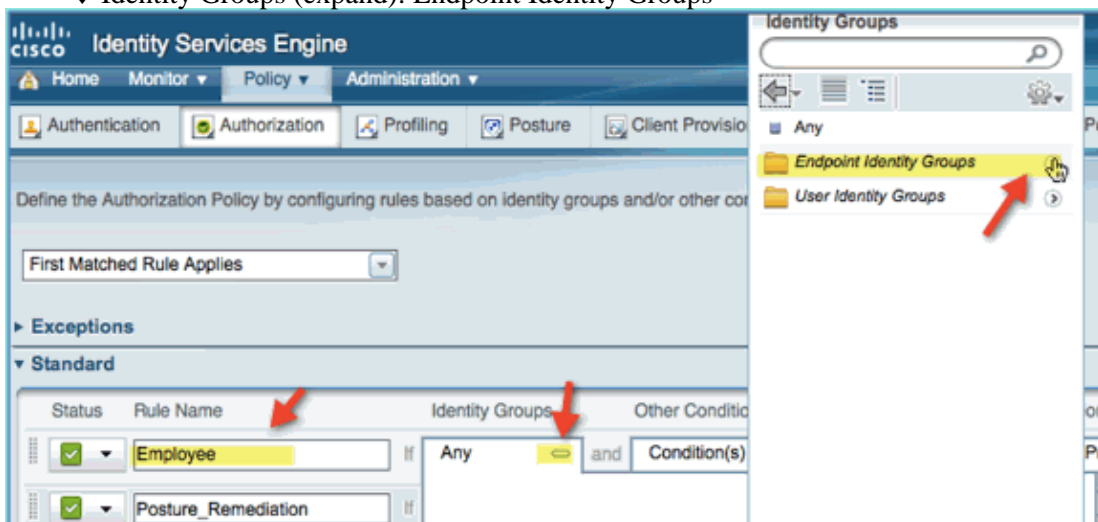
Complete these steps:

1. Navigate to **ISE > Policy > Authorization**.
2. Add/Insert a new rule above the Posture Remediation policy/line.

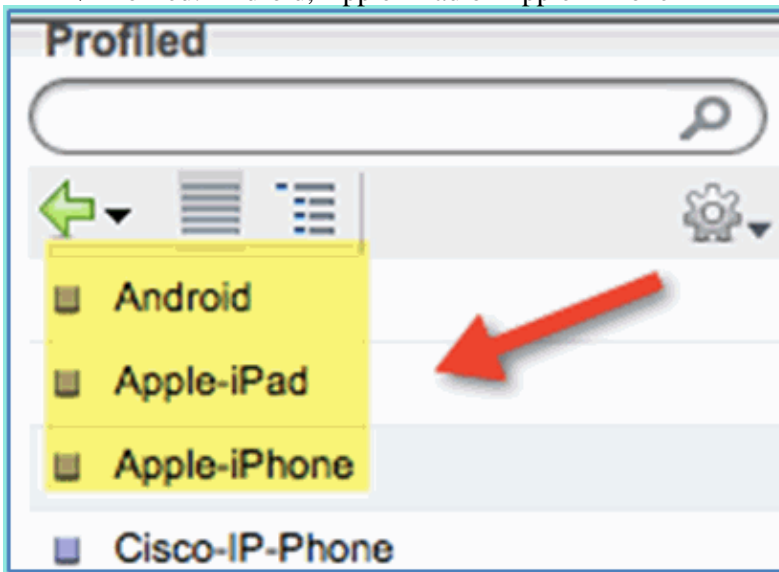


3. Enter the following values for this policy:

- ◆ Rule Name: Employee
- ◆ Identity Groups (expand): Endpoint Identity Groups

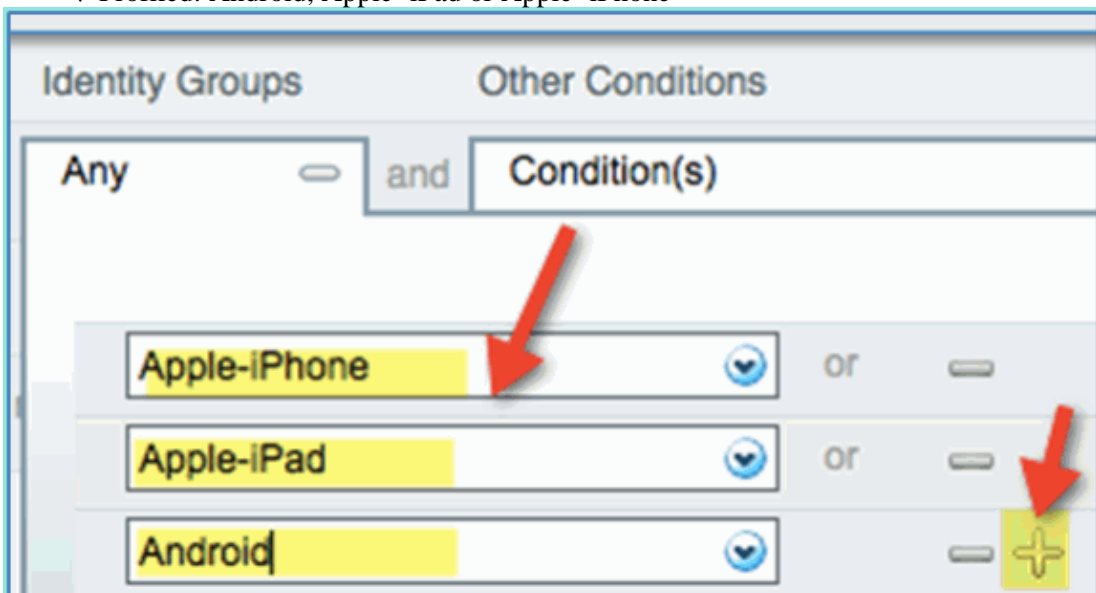


- ◆ Endpoint Identity Groups: Profiled
- ◆ Profiled: Android, Apple-iPad or Apple-iPhone



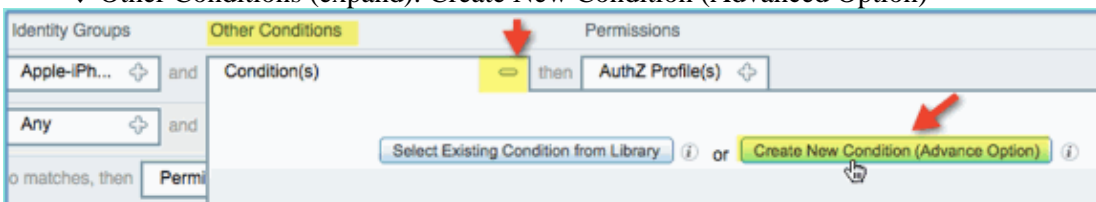
4. In order to specify additional device types, click the + and add more devices (if needed):

- ◆ Endpoint Identity Groups: Profiled
- ◆ Profiled: Android, Apple-iPad or Apple-iPhone

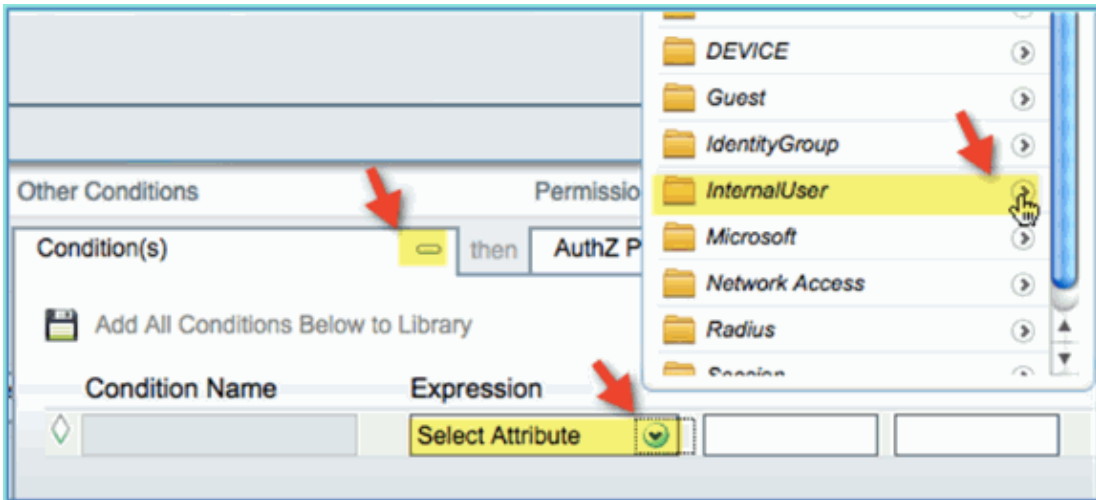


5. Specify the following Permissions values for this policy:

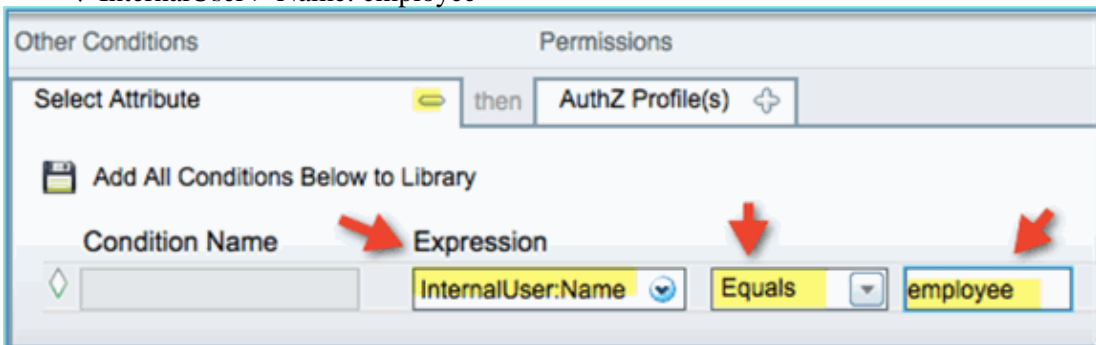
- ◆ Other Conditions (expand): Create New Condition (Advanced Option)



- ◆ Condition > Expression (from list): InternalUser > Name

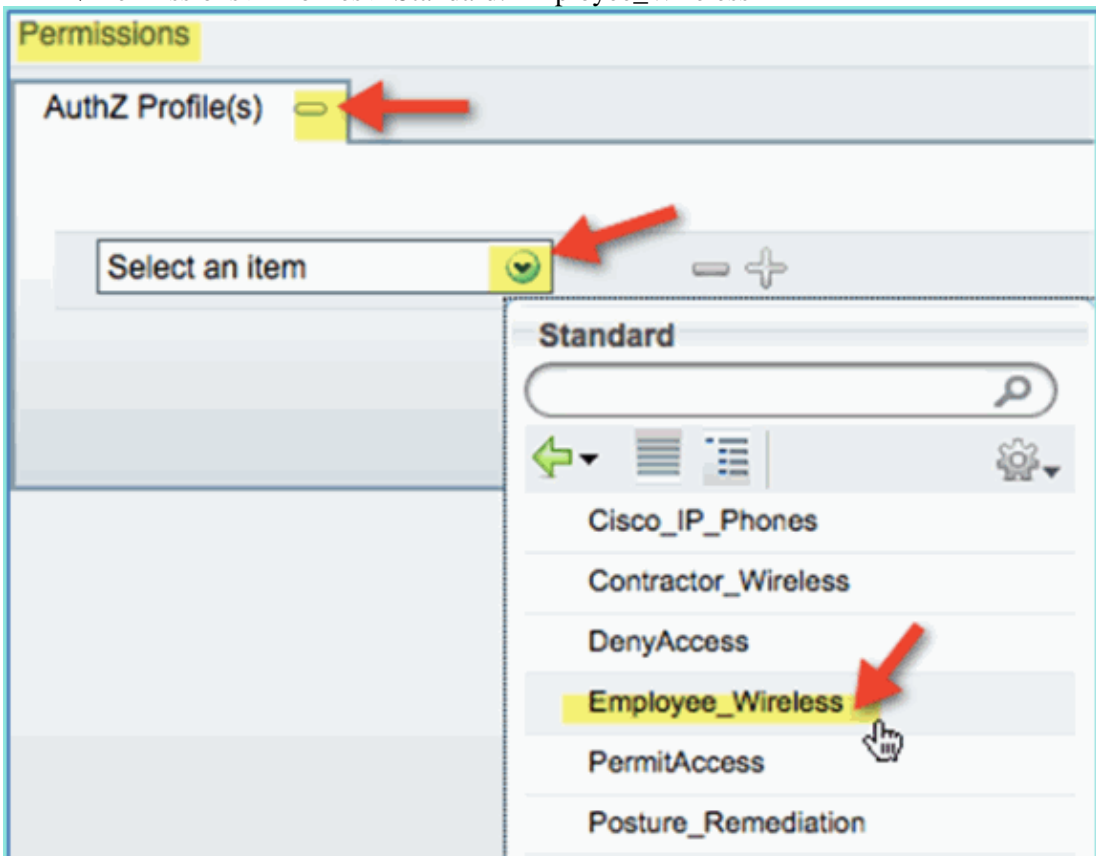


◆ InternalUser > Name: employee

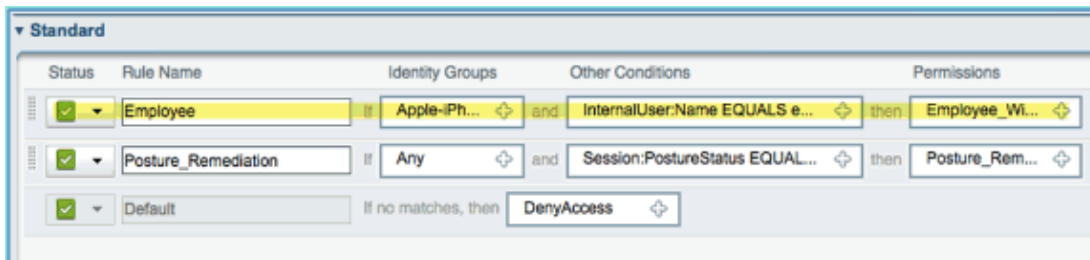


6. Add a condition for posture session Compliant:

◆ Permissions > Profiles > Standard: Employee_Wireless

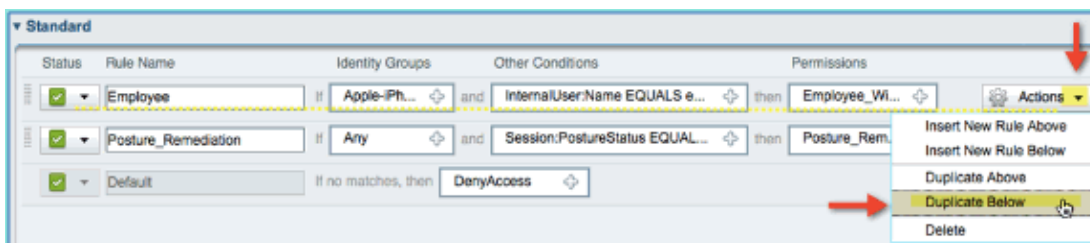


7. Click **Save**. Confirm that the policy has been added properly.



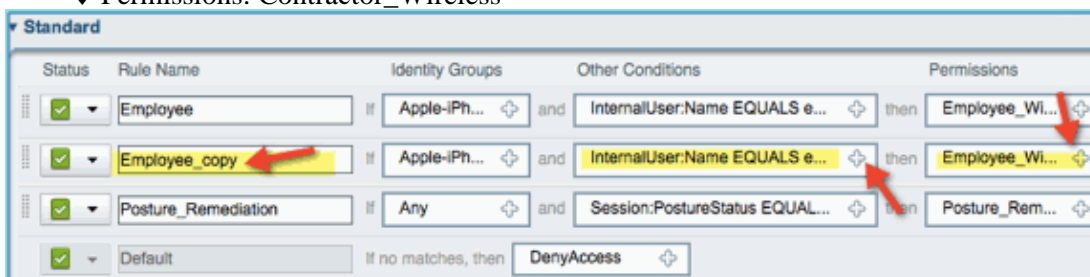
8. Continue by adding the Contractor policy. In this document, the previous policy is duplicated in order to expedite the process (or, you can manually configure for good practice).

From the Employee policy > Actions, click **Duplicate Below**.

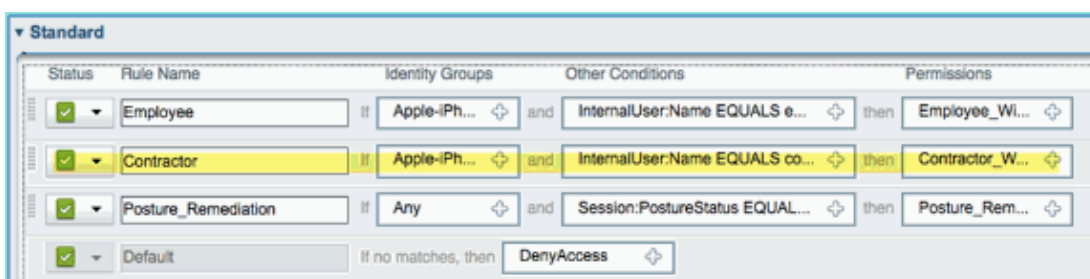


9. Edit the following fields for this policy (duplicate copy):

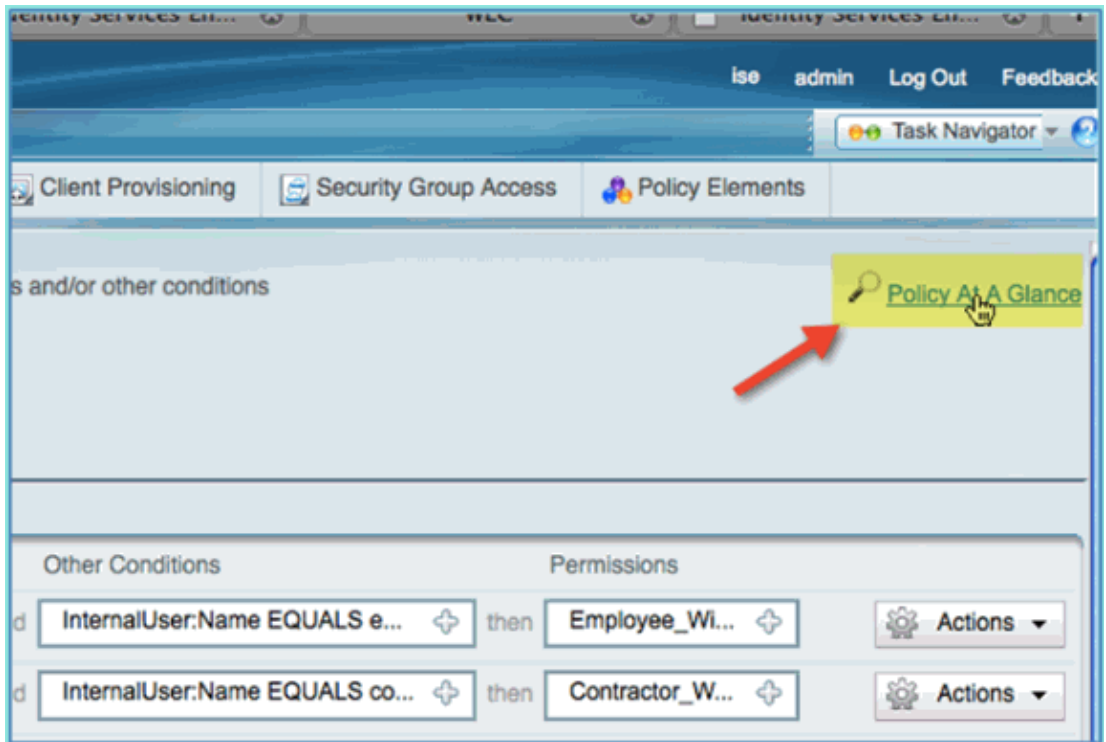
- ◆ Rule Name: Contractor
- ◆ Other Conditions > InternalUser > Name: contractor
- ◆ Permissions: Contractor_Wireless



10. Click **Save**. Confirm that the previous duplicated copy (or new policy) is configured properly.



11. In order to preview the policies, click **Policy-at-a-Glance**.



Policy at A Glance view provides a consolidated summarized and easy to see policies.

Authorization Policy At A Glance				
First Matched Rule Applies				
Exceptions				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
			No data available	
Standard				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
Enabled	Employee	Android OR Apple-iPad OR Apple- iPhone	InternalUser:Name EQUALS employee	Employee_Wireless
Enabled	Contractor	Android OR Apple-iPad OR Apple- iPhone	InternalUser:Name EQUALS contractor	Contractor_Wireless
Enabled	Posture_Remediation	Any	Session:PostureStatus EQUALS Unknown	Posture_Remediation
Enabled	Default	Any		DenyAccess

Testing CoA for Differentiated Access

With the authorization profiles and policies prepared for differentiating access, it is time to test. Having a single secured WLAN, an employee will be assigned the employee VLAN and a contractor will be for the contractor VLAN. An Apple iPhone/iPad is used in the next examples.

Complete these steps:

1. Connect to the secured WLAN (POD1x) with the mobile device and use these credentials:

- ◆ Username: employee
- ◆ Password: XXXXX

Enter the password for "pod1x"

Cancel **Enter Password**

Username employee

Password ●●●●●●3

Mode Automatic >

1 2 3 4 5 6 7 8 9 0

2. Click **Join**. Confirm that the employee is assigned VLAN 11 (Employee VLAN).



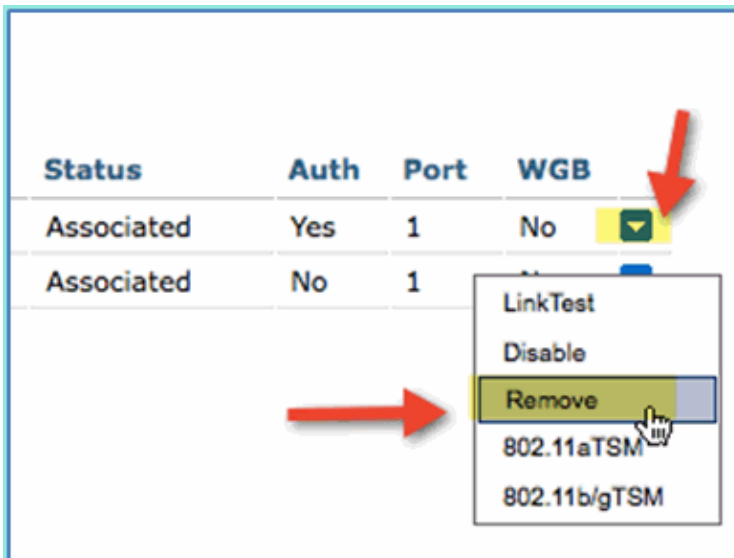
3. Click **Forget this Network**. Confirm by clicking **Forget**.



4. Go to WLC and remove existing client connections (if the same was used in previous steps). Navigate to **Monitor > Clients > MAC address**, then click **Remove**.



The screenshot shows the Cisco WLC interface. At the top, there is a navigation bar with the Cisco logo and two tabs: "MONITOR" (highlighted in green) and "WLANs". Below the navigation bar, the "Monitor" section is active, showing a sidebar with options: Summary, Access Points, Cisco CleanAir, Statistics, CDP, Rogues, Clients (highlighted in yellow), and Multicast. A red arrow points to the "Clients" link in the sidebar. The main content area is titled "Clients" and includes a "Current Filter" section with two entries: "Client MAC Addr" with values "44:2a:60:f7:3a:4a" and "5c:59:48:40:82:8d".



The screenshot shows a table of client sessions. The table has columns for Status, Auth, Port, and WGB. A red arrow points to a dropdown menu icon in the WGB column of the first row. The dropdown menu is open, showing options: LinkTest, Disable, Remove (highlighted), 802.11aTSM, and 802.11b/gTSM. Another red arrow points to the "Remove" option.

Status	Auth	Port	WGB
Associated	Yes	1	No <input checked="" type="checkbox"/>
Associated	No	1	

5. Another sure way to clear previous client sessions is to disable/enable the WLAN.

- a. Go to **WLC > WLANs > WLAN**, then click the WLAN to edit.
- b. Un-check **Enabled > Apply** (to disable).
- c. Check the box for **Enabled > Apply** (to re-enable).



6. Go back to the mobile device. Connect again to the same WLAN with these credentials:

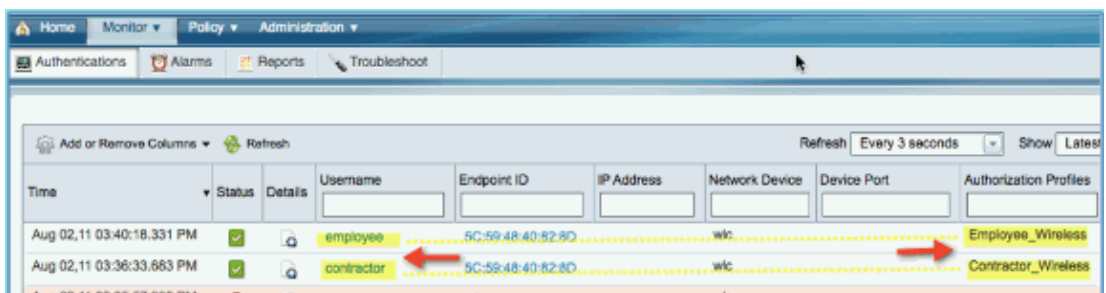
- ◆ Username: contractor
- ◆ Password: XXXX



7. Click **Join**. Confirm that the contractor user is assigned VLAN 12 (Contractor/guest VLAN).



8. You can look at ISE real-time log view in **ISE > Monitor > Authorizations**. You should see individual users (employee, contractor) get differentiated authorization profiles (Employee_Wireless vs Contractor_Wireless) in different VLANs.



WLC Guest WLAN

Complete these steps in order to add a guest WLAN to allow guests to access the ISE Sponsor Guest Portal:

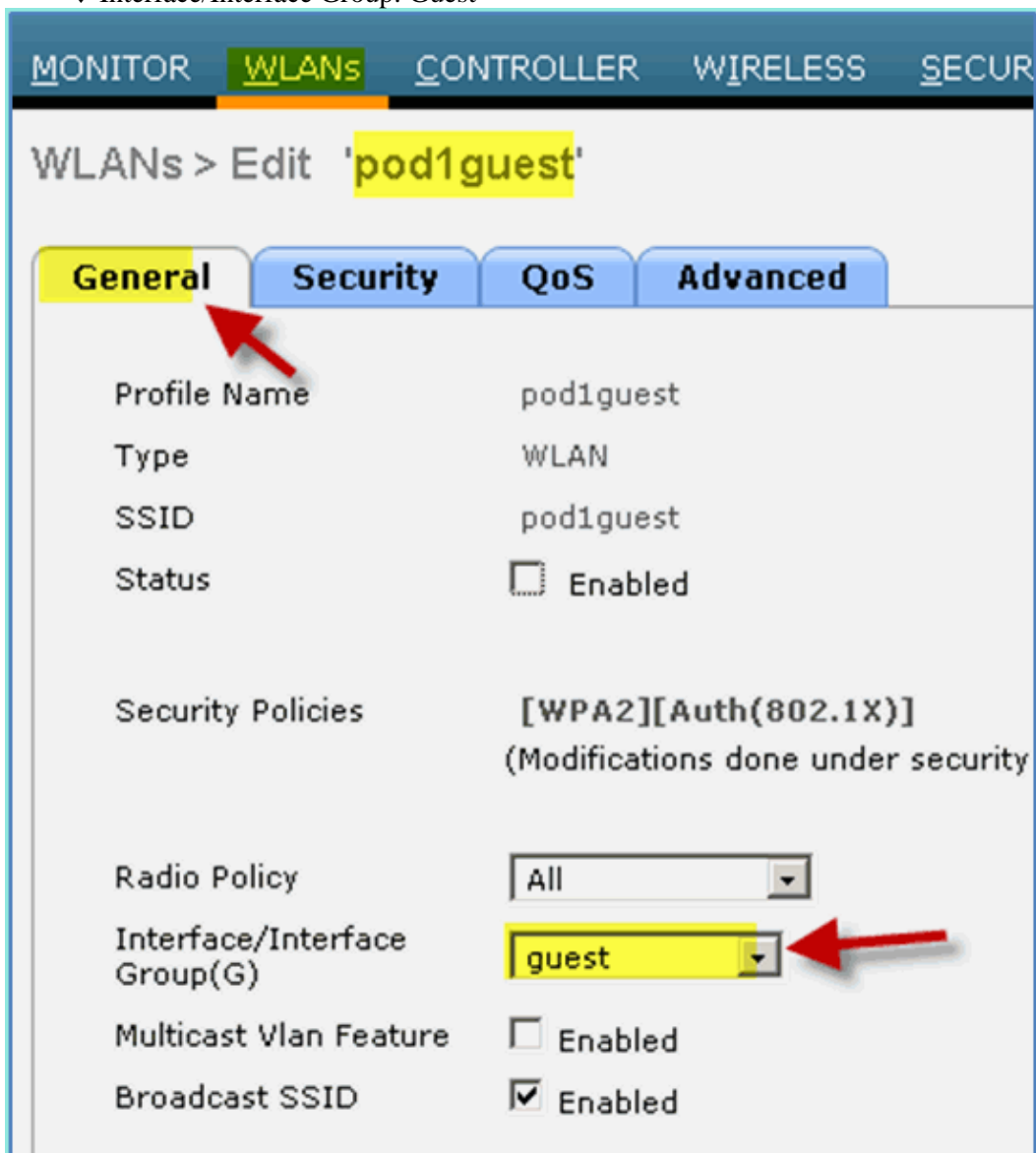
1. From WLC, navigate to **WLANs > WLANs > Add New**.
2. Enter the following for the new guest WLAN:
 - ◆ Profile Name: pod1guest
 - ◆ SSID: pod1guest



3. Click **Apply**.

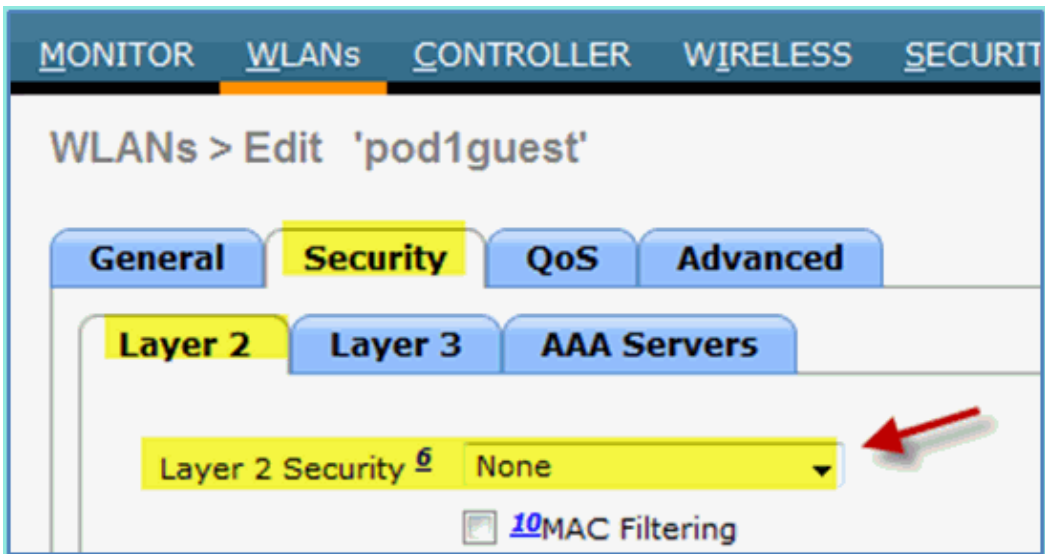
4. Enter the following under the guest WLAN > General tab:

- ◆ Status: Disabled
- ◆ Interface/Interface Group: Guest



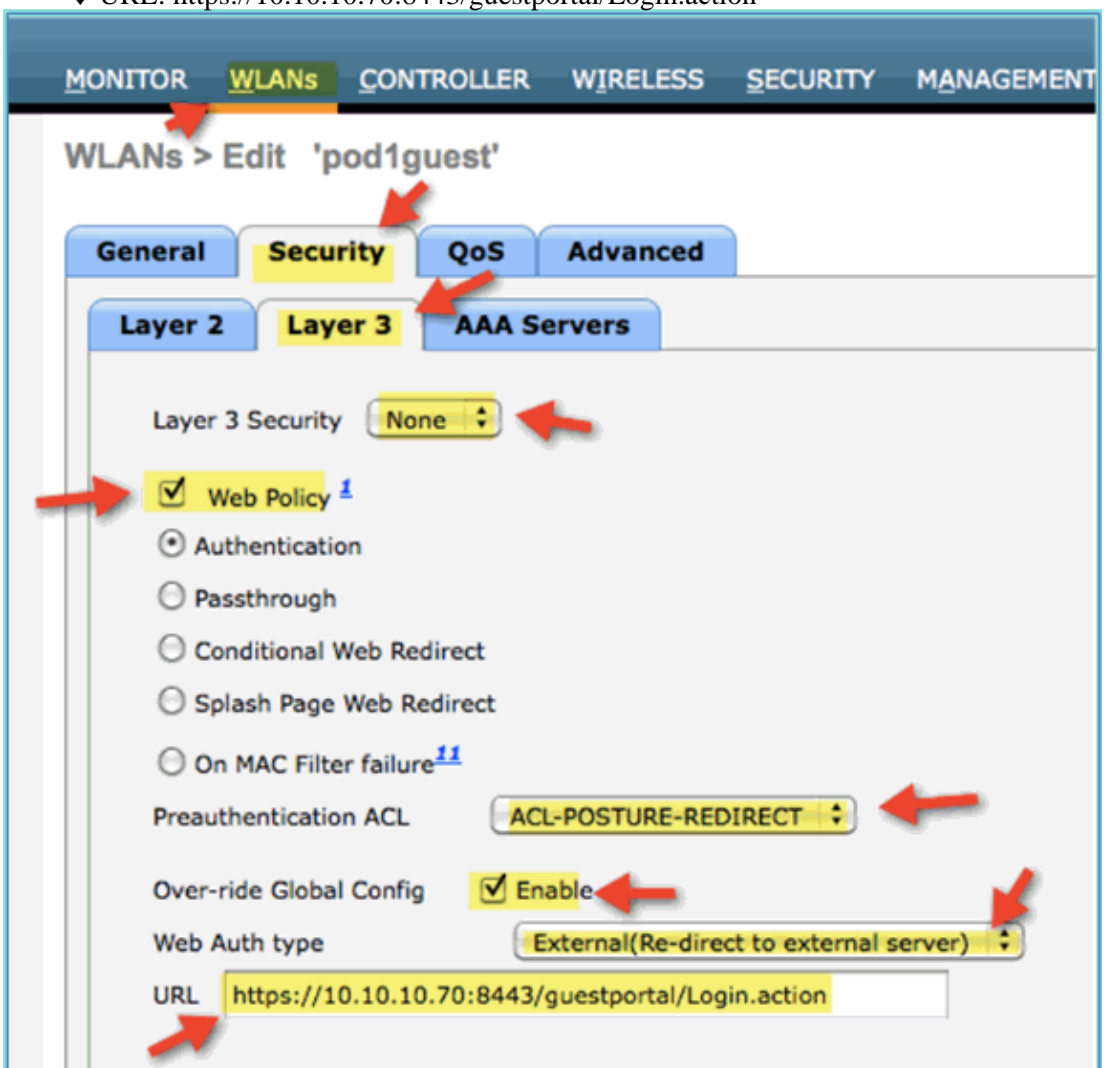
5. Navigate to guest WLAN > Security > Layer2 and enter the following:

- ◆ Layer 2 Security: None



6. Navigate to guest WLAN > Security > Layer3 tab and enter the following:

- ◆ Layer 3 Security: None
- ◆ Web Policy: Enabled
- ◆ Web Policy sub value: Authentication
- ◆ Preauthentication ACL: ACL-POSTURE-REDIRECT
- ◆ Web Auth type: External (Re-direct to external server)
- ◆ URL: https://10.10.10.70:8443/guestportal/Login.action



7. Click **Apply**.
8. Make sure to **save the WLC Configuration**.

Testing the Guest WLAN and Guest Portal

Now, you can test the configuration of the guest WLAN. It should redirect the guests to the ISE guest portal.

Complete these steps:

1. From an iOS device such as an iPhone, navigate to **Wi-Fi Networks > Enable**. Then, select the POD guest network.



2. Your iOS device should show a valid IP address from the guest VLAN (10.10.12.0/24).

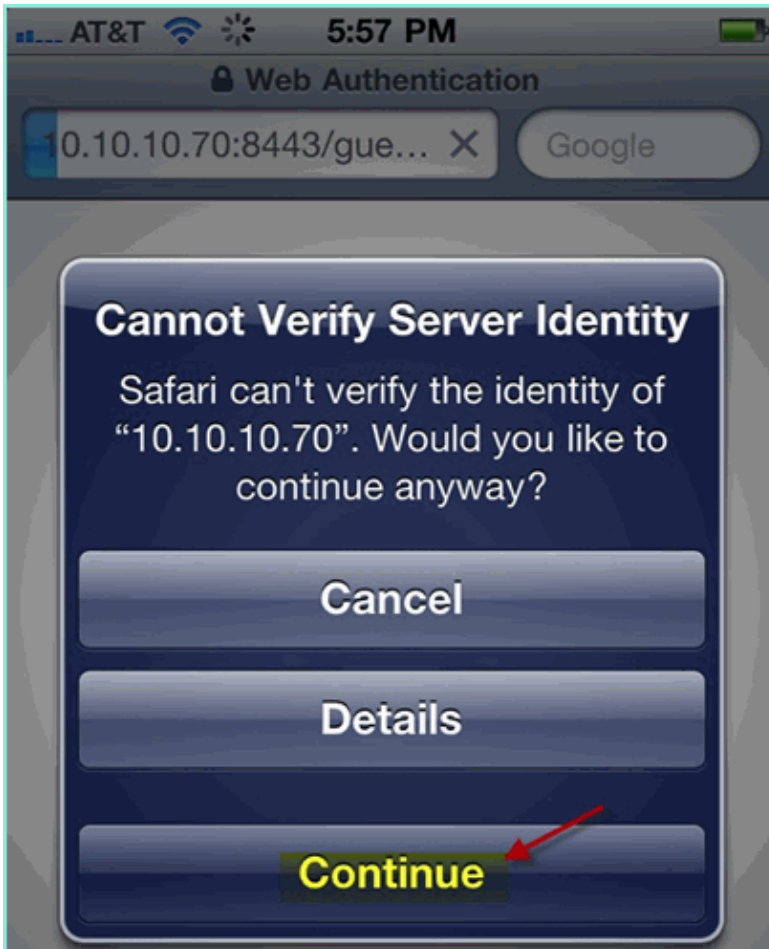


3. Open the Safari browser and connect to:

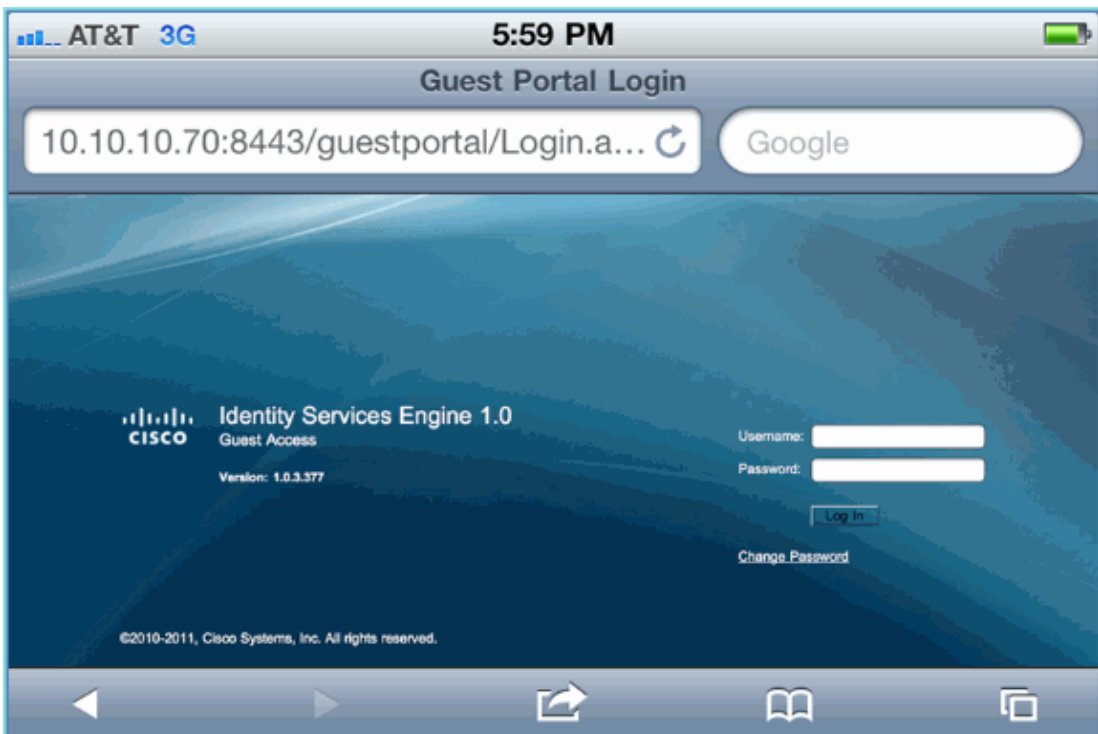
◆ URL: <http://10.10.10.10>

A Web Authentication redirect appears.

4. Click **Continue** until you have arrived at the ISE Guest Portal page.



The next sample screenshot shows the iOS device on a Guest Portal Login. This confirms that the correct setup for the WLAN and ISE Guest Portal is active.

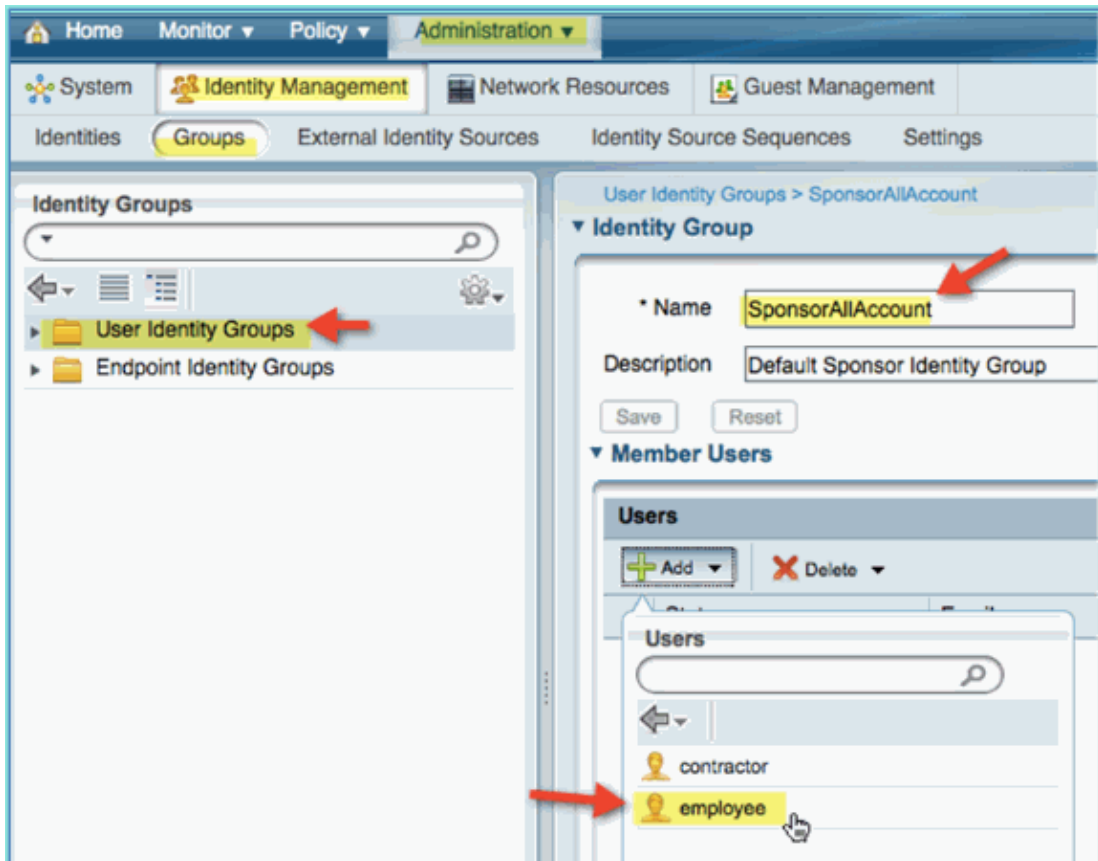


ISE Wireless Sponsored Guest Access

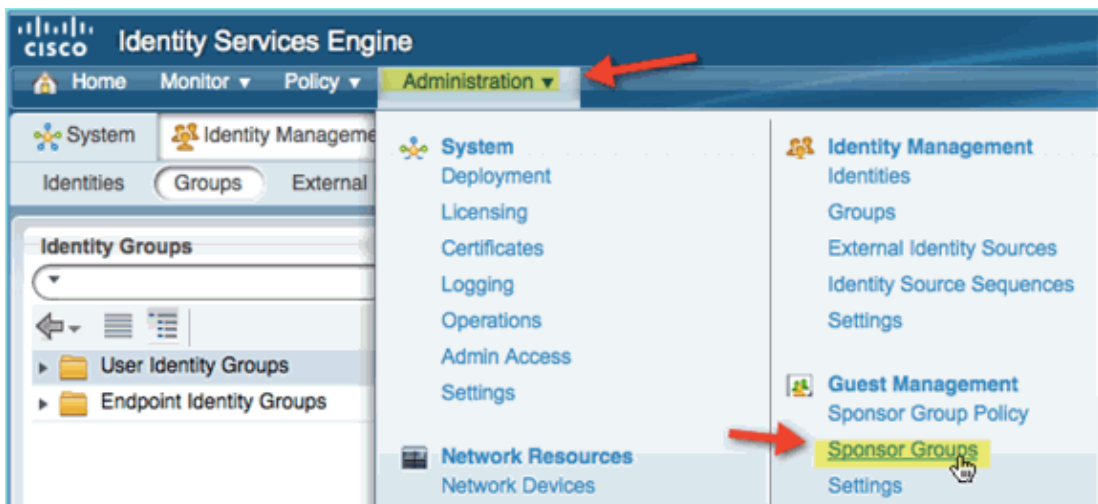
ISE can be configured to allow guests to be sponsored. In this case you will configure ISE guest policies to allow either Internal or AD domain (if integrated) users to sponsor guest access. You will also configure ISE to allow sponsors to view guest password (optional), which is helpful to this lab.

Complete these steps:

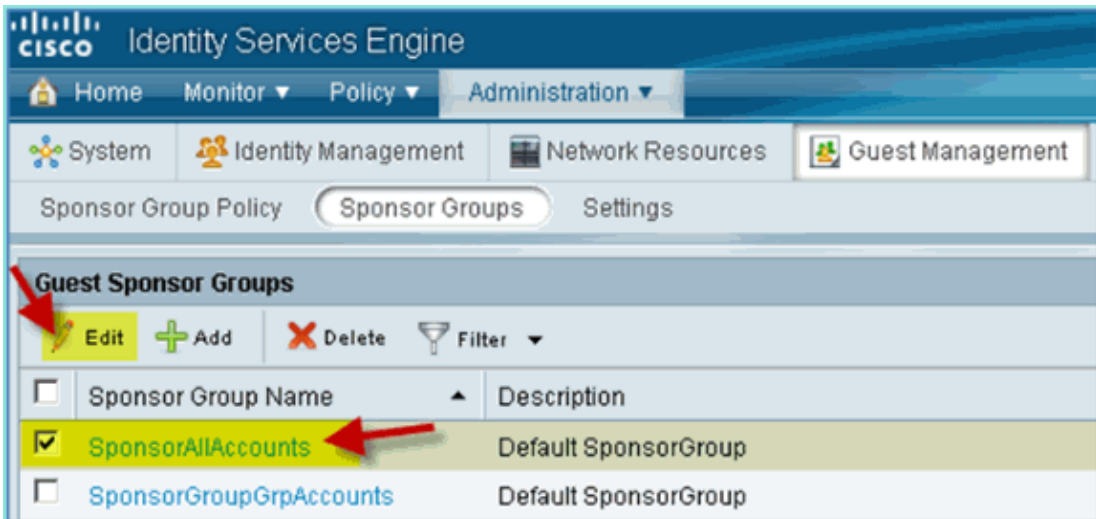
1. Add employee user to the SponsorAllAccount group. There are different ways to do this: go directly to the group, or edit the user and assign group. For this example, navigate to **Administration > Identity Management > Groups > User Identity Groups**. Then, click **SponsorAllAccount** and add employee user.



2. Navigate to **Administration > Guest Management > Sponsor Groups**.

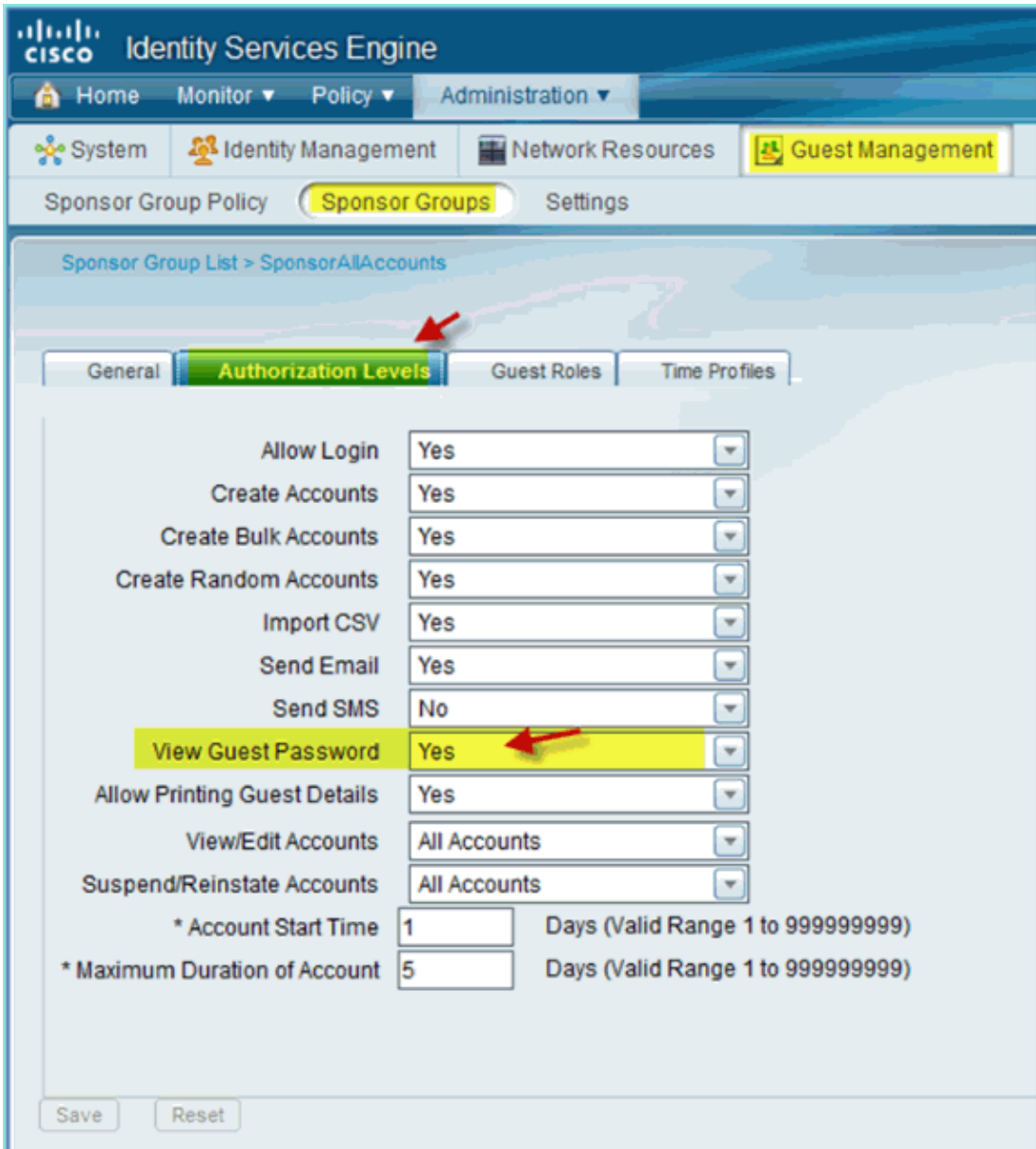


3. Click **Edit**, then choose **SponsorAllAccounts**.



4. Select Authorization Levels and set the following:

- ◆ View Guest Password: Yes



5. Click **Save** in order to complete this task.

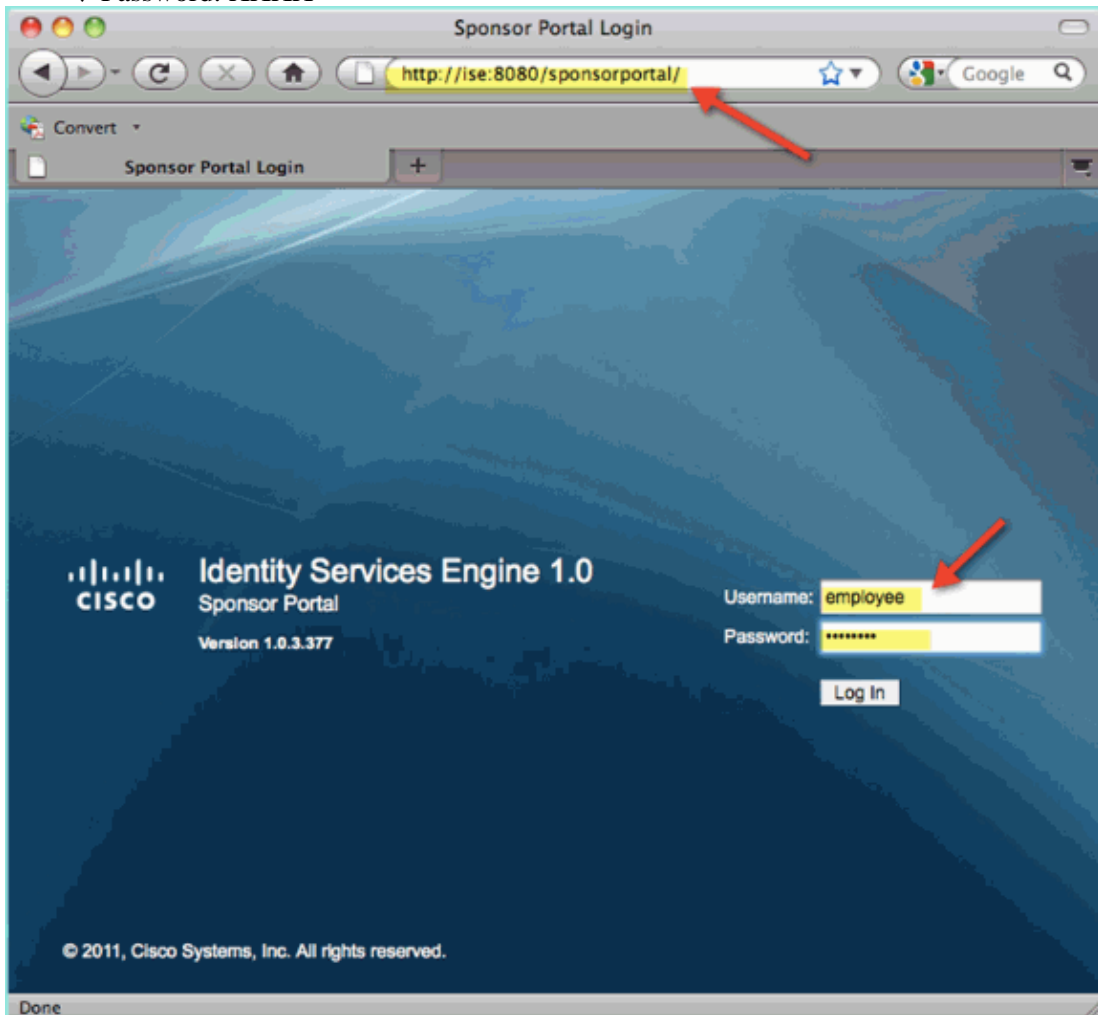
Sponsoring Guest

Previously, you have configured the appropriate guest policy and groups to allow AD domain user to sponsor temporary guests. Next, you will access the Sponsor Portal and create a temporary guest access.

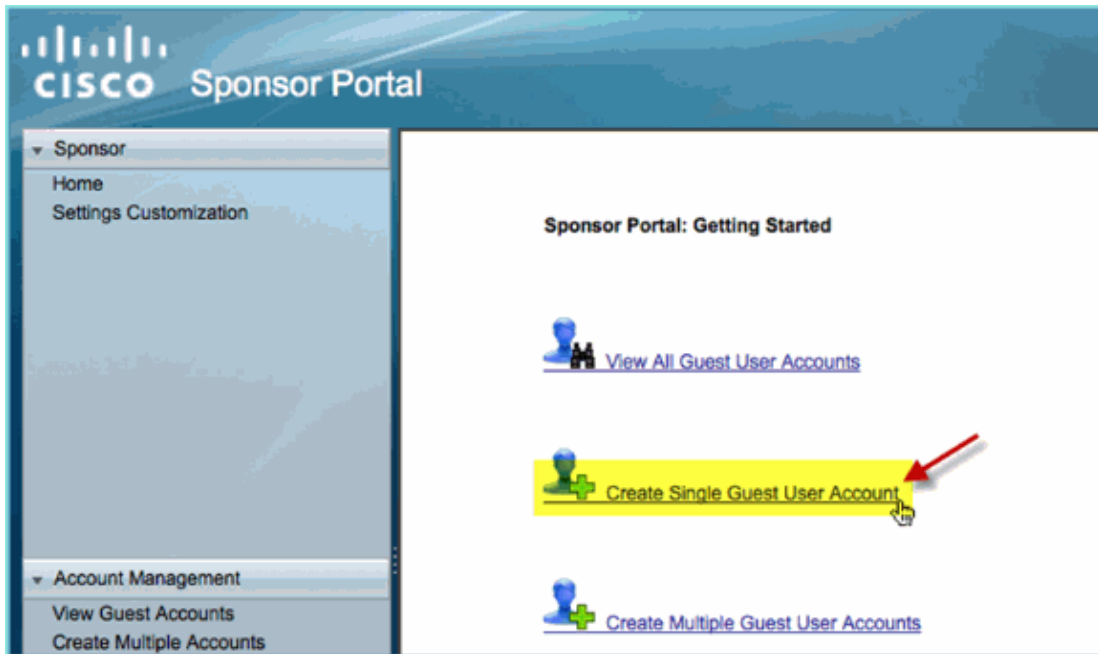
Complete these steps:

1. From a browser, navigate to either of these URLs: <http://<ise ip>:8080/sponsorportal/> **or** <https://<ise ip>:8443/sponsorportal/>. Then, log in with the following:

- ◆ Username: aduser (Active Directory), employee (Internal User)
- ◆ Password: XXXX



2. From the Sponsor page, click **Create Single Guest User Account**.



3. For a temporary guest, add the following:

- ◆ First Name: Required (for example, Sam)
- ◆ Last Name: Required (for example, Jones)
- ◆ Group Role: Guest
- ◆ Time Profile: DefaultOneHour
- ◆ Time Zone: Any/Default

Sponsor Portal

Account Management > [View All Guest Accounts](#) > Create Guest Account

Create Guest Account

First Name:

Last Name:

Email Address:

Phone Number:

Company:

Optional Data 1:

Optional Data 2:

Optional Data 3:

Optional Data 4:

Optional Data 5:

Group Role:


Time Profile:

Timezone:

⚙ = Required fields

4. Click **Submit**.
5. A guest account is created based on your previous entry. Note that the password is visible (from previous exercise) as opposed to hash ***.
6. Leave this window open showing the Username and Password for the guest. You will use them to test Guest Portal Login (next).

Account Management > [View All Guest Accounts](#) > Create Guest Account

 **Successfully Created Guest Account siam0002**

Username: siam0002
Password: 5_5g6d7Kx
First Name: Sam
Last Name: iAm
Email Address:
Phone Number:
Company:
Status: AWAITING INITIAL LOGIN
Suspended: false
Optional Data 1:
Optional Data 2:
Optional Data 3:
Optional Data 4:
Optional Data 5:
Group Role: Guest
Time Profile: DefaultOneHour

Timezone: EST
Account Start Date: 2011-07-15 13:56:04 EST
Account Expiration Date: 2011-07-15 14:56:04 EST

[Email](#) [Print](#) [Create Another Account](#) [View All Accounts](#)

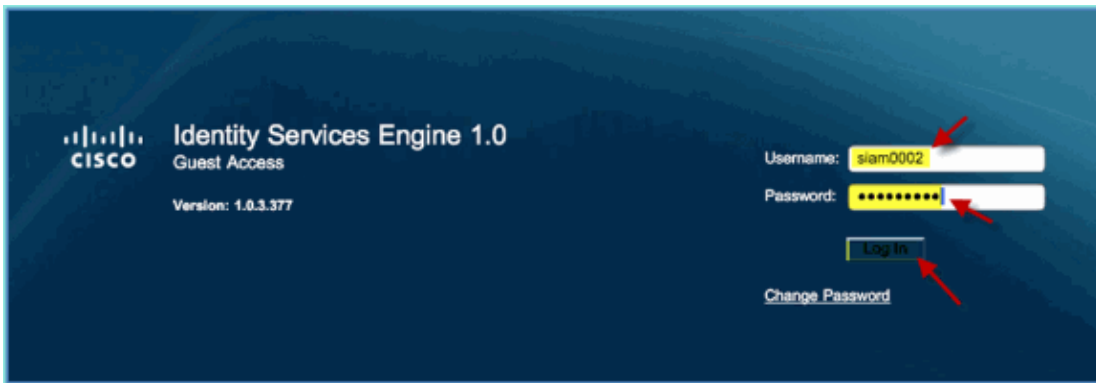
Testing Guest Portal Access

With the new guest account created by an AD user/sponsor, it is time to test the guest portal and access.

Complete these steps:

1. On a preferred device (in this case an Apple iOS / iPad), connect to the Pod Guest SSID and check IP address /connectivity.
2. Use the browser and attempt to navigate to <http://www>.

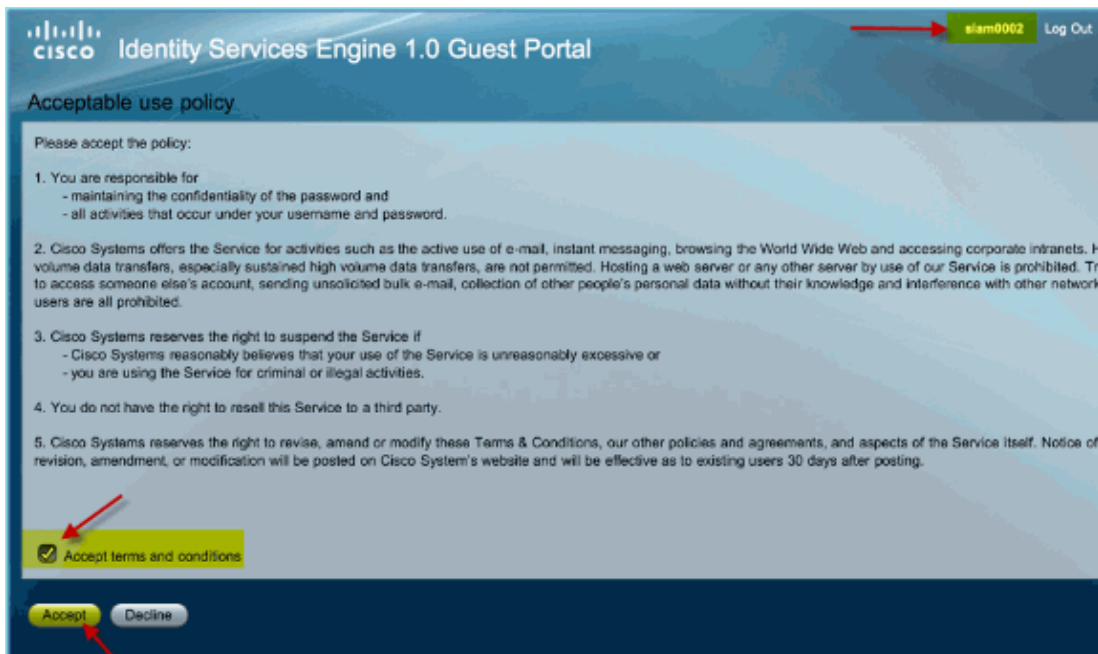
You are redirected to the Guest Portal Login page.



3. Log in using the guest account created in the previous exercise.

If successful, the Acceptable use policy page appears.

4. Check **Accept terms and conditions**, then click **Accept**.



The original URL is completed, and the endpoint is permitted access as guest.

Certificate Configuration

In order to secure communications with ISE, determine whether the communication is authentication related or for ISE management. For example, for configuration using the ISE web UI, X.509 certificates and certificate trust chains need to be configured to enable asymmetric encryption.

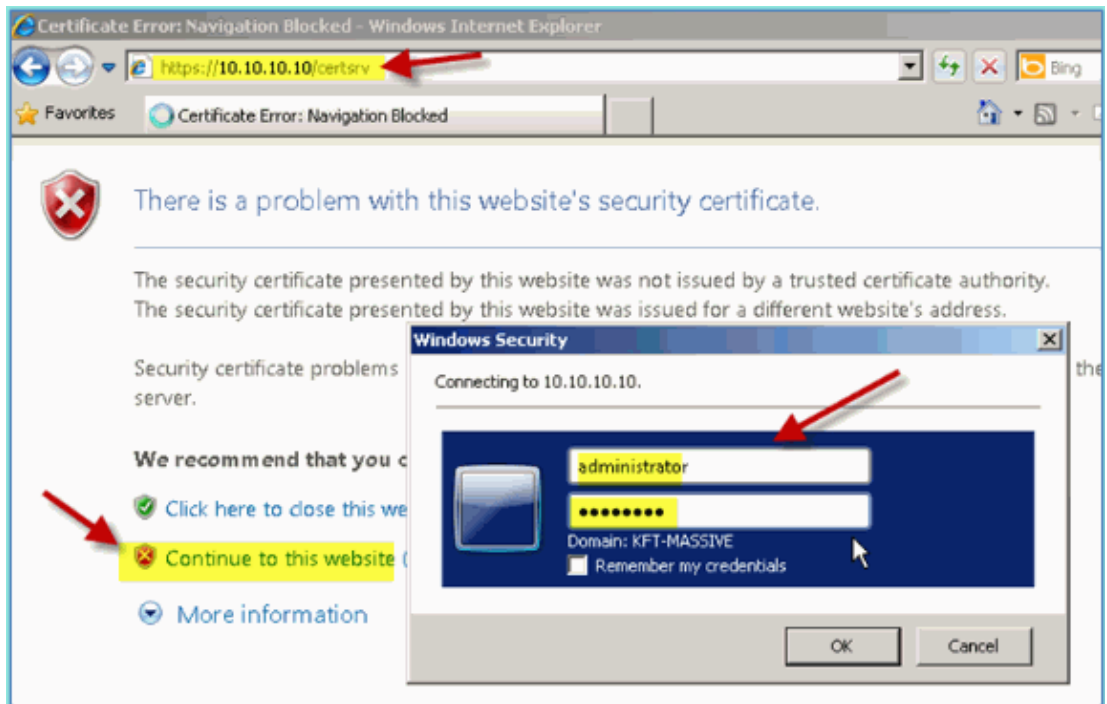
Complete these steps:

1. From your wired connected PC, open a browser window to <https://AD/certsrv>.

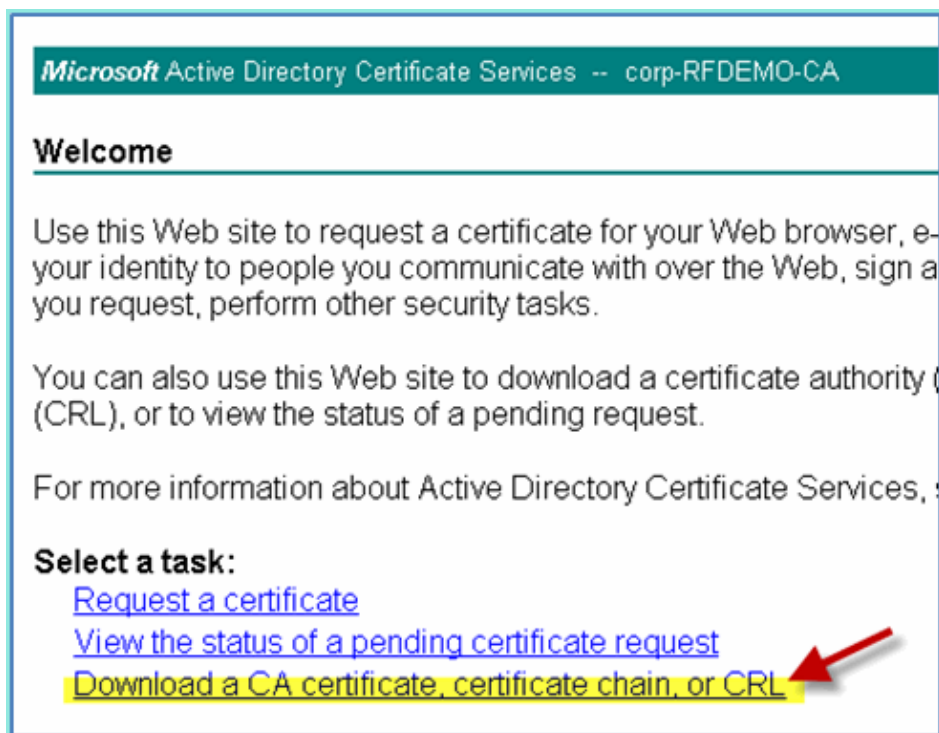
Note: Use the secure HTTP.

Note: Use Mozilla Firefox or MS Internet Explorer in order to access ISE.

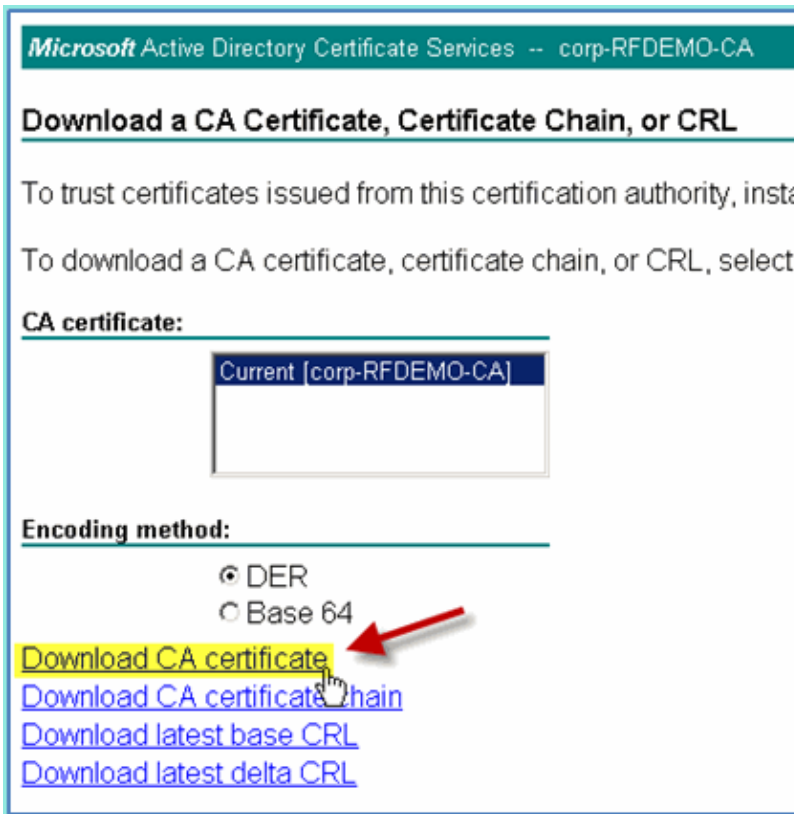
2. Log in as administrator/Cisco123.



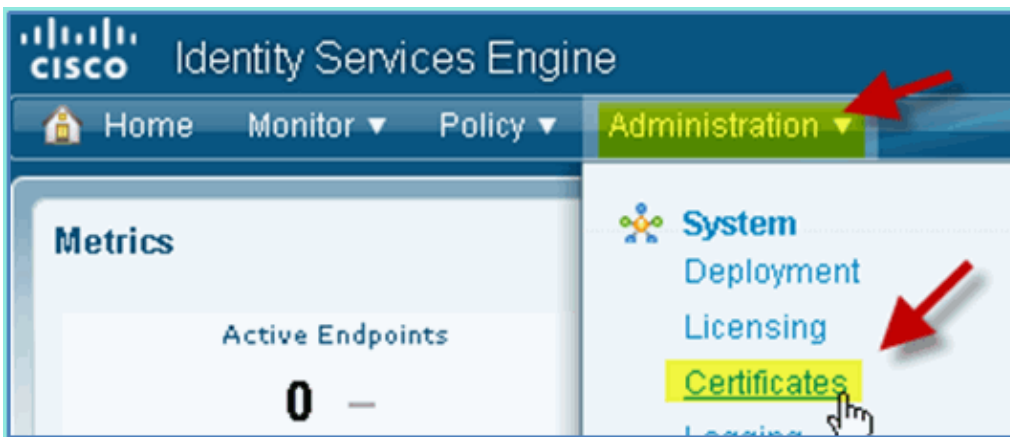
3. Click **Download a CA certificate, certificate chain, or CRL**.



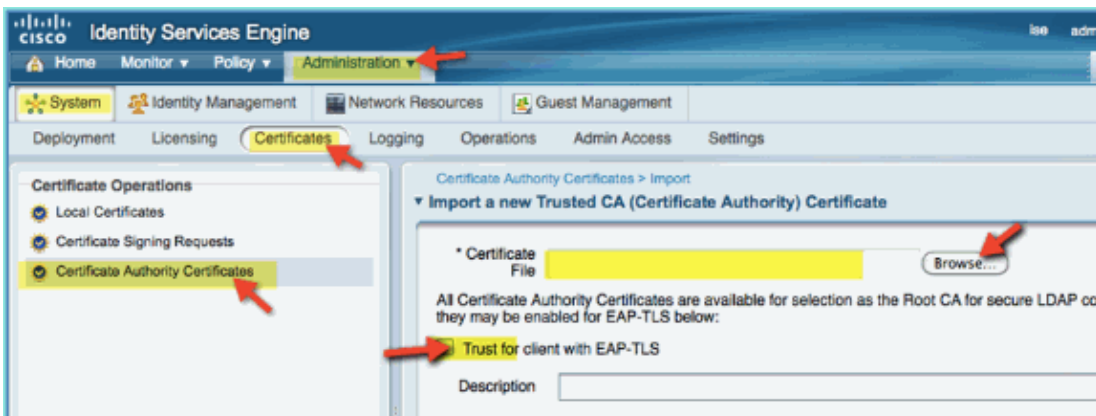
4. Click **Download CA certificate** and save it (note the save location).



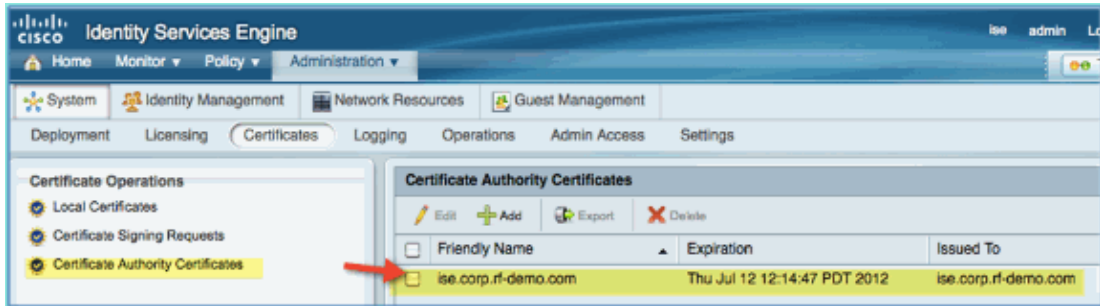
5. Open a browser window to <https://<Pod-ISE>>.
6. Go to **Administration > System > Certificates > Certificates Authority Certificates**.



7. Select **Certificate Authority Certificates** operation and browse to the previously downloaded CA cert.
8. Select **Trust for client with EAP-TLS**, then submit.

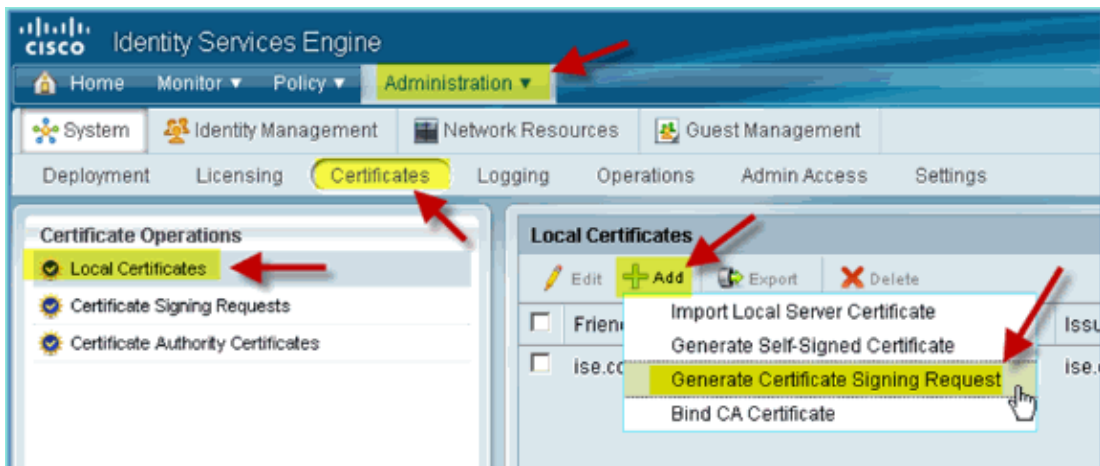


9. Confirm that the CA has been added trusted as root CA.



10. From a browser, go to **Administration > System > Certificates > Certificates Authority Certificates**.

11. Click **Add**, then **Generate Certificate Signing Request**.



12. Submit these values:

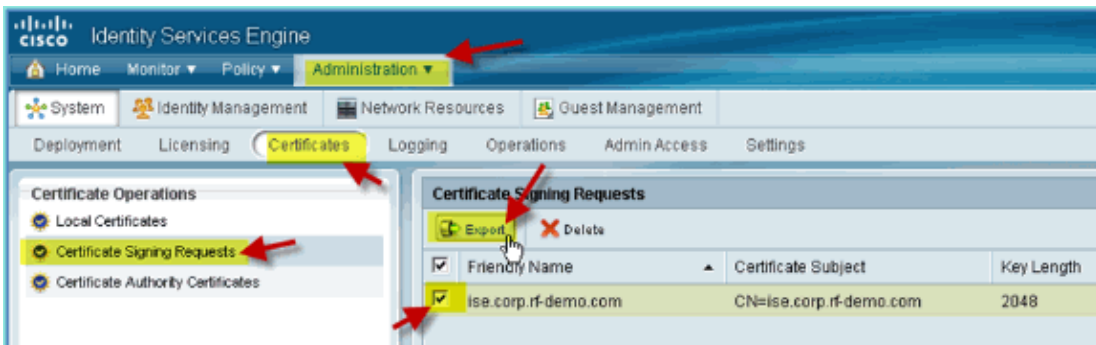
- ◆ Certificate Subject: CN=ise.corp.rf-demo.com
- ◆ Key Length: 2048



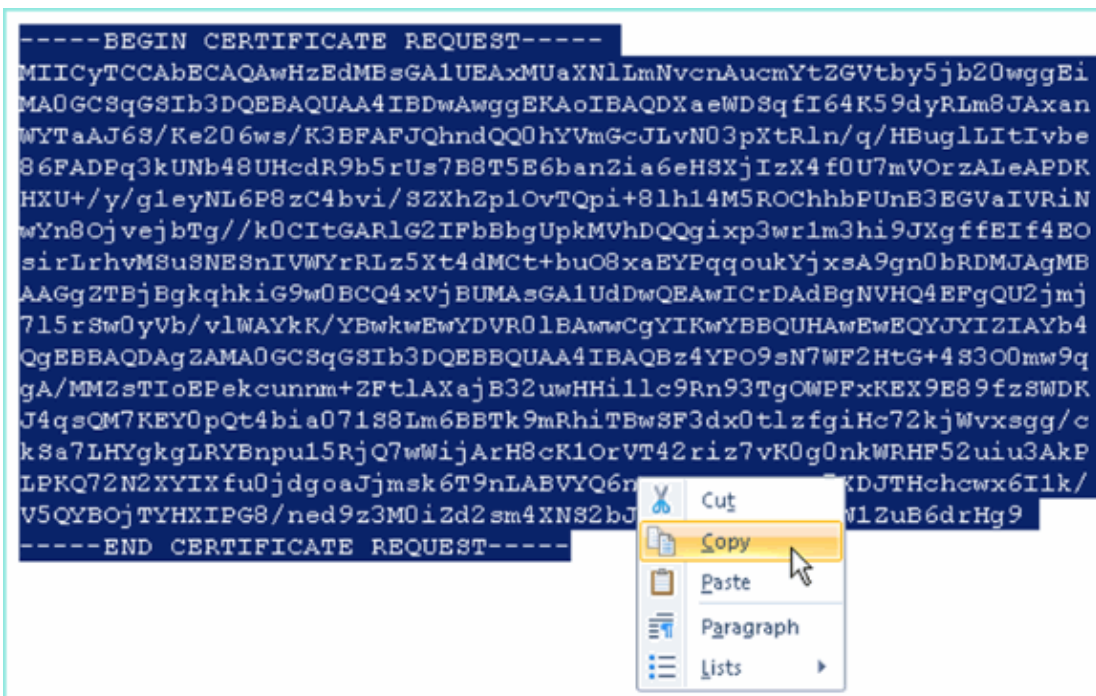
13. ISE prompts that the CSR is available in the CSR page. Click **OK**.



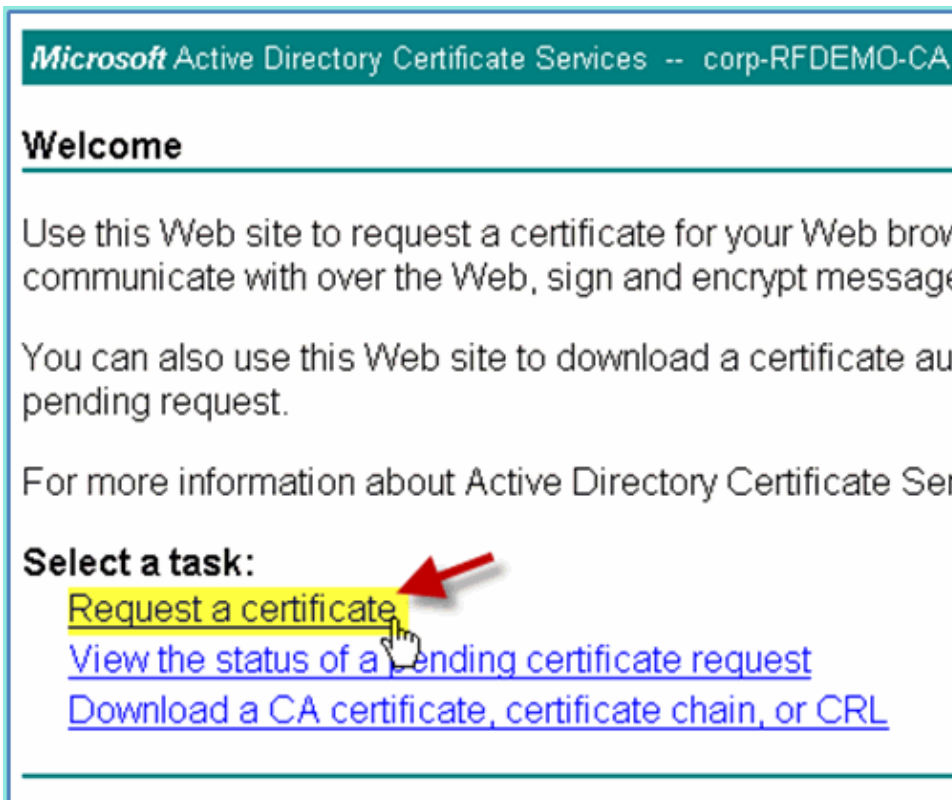
14. Select the CSR from the ISE CSR page and click **Export**.
15. Save the file to any location (for example, Downloads, etc.)
16. File will be saved as *.pem.



17. Locate the CSR file and edit with either Notepad/Wordpad/TextEdit.
18. Copy the content (Select all > Copy).



19. Open a browser window to <https://<Pod-AD>/certsrv>.
20. Click **Request a certificate**.



21. Click to submit an **advanced certificate request**.



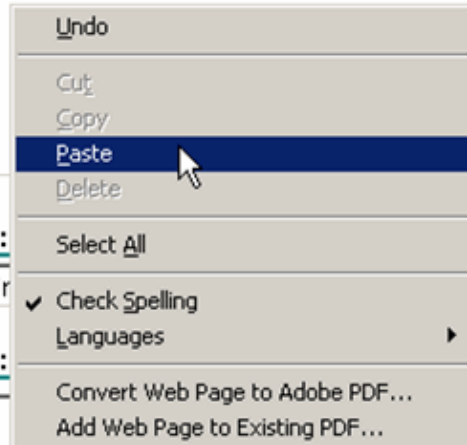
22. Paste the CSR content in the Saved Request Field.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CM source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):



Certificate Template:

Adr

Additional Attributes:

Attributes:

23. Select **Web Server** as the Certificate Template, then click **Submit**.

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CM source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
gA/MMZsTioEPEkcunm+ZFt1AXajB32uwHH11c9
J4qsQM7KEYOpQt4bia071S8Lm6BBTk9mRhiTBwSF
kSa7LHYgkgLRYBnpu15RjQ7wWijArH8cK1OrVT42
LPKQ72N2XYIXfu0jdgaoAjmsk6T9nLABVYQ6nKQx
V5QYBOjTYHXIPG8/ned9z3M0iZd2sm4XNS2bJfO/
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit


24. Select **DER encoded**, then click **Download certificate**.

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

Certificate Issued

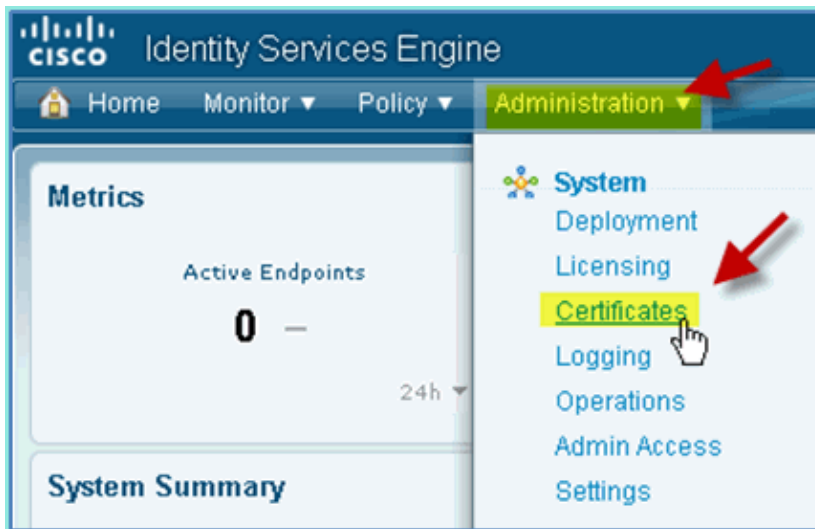
The certificate you requested was issued to you.

DER encoded or Base 64 encoded

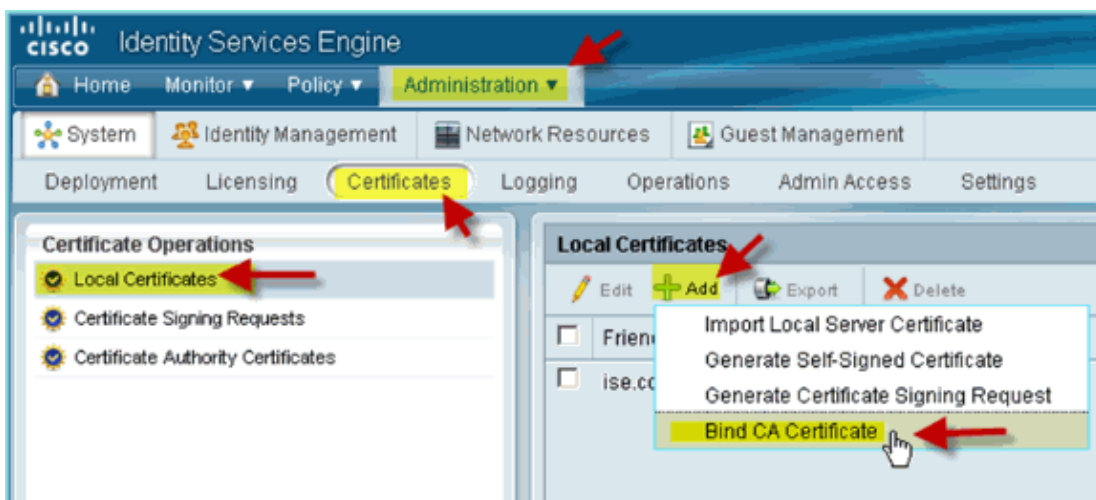
 [Download certificate](#) [Download certificate chain](#)

25. Save the file to a known location (for example, Downloads)

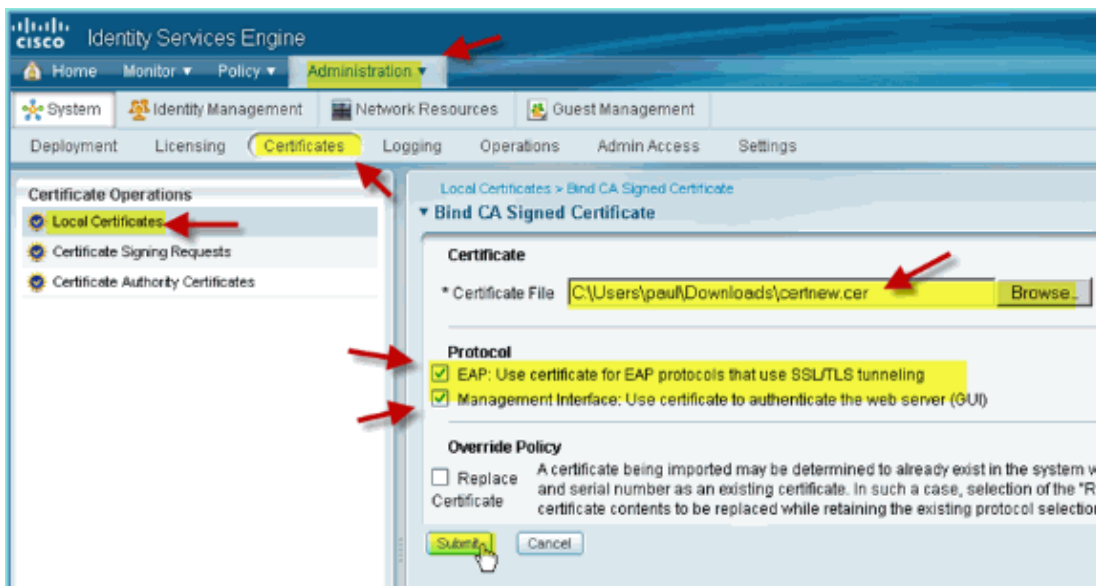
26. Go to **Administration > System > Certificates > Certificates Authority Certificates**.



27. Click **Add** > **Bind CA Certificate**.

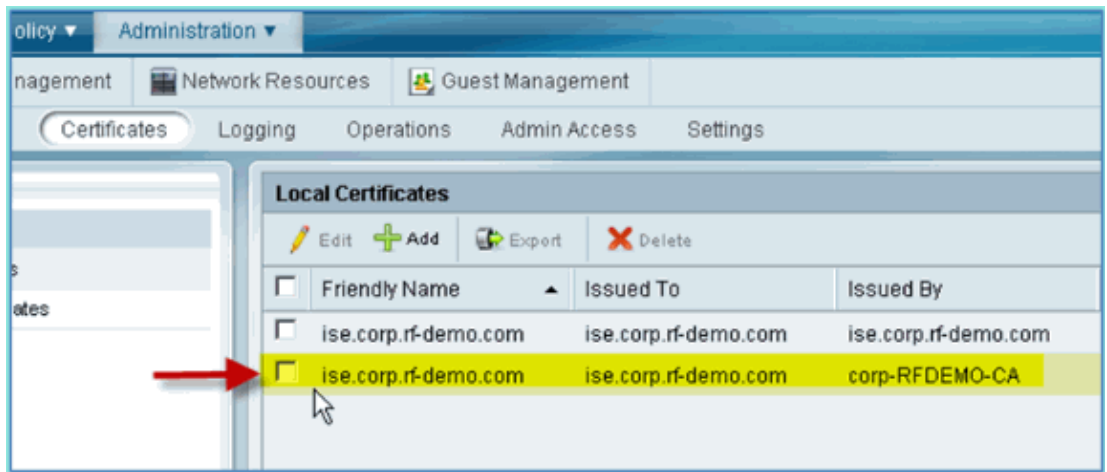


28. Browse to the previously downloaded CA certificate.



29. Select both **Protocol EAP** and **Management Interface**, then click **Submit**.

30. Confirm that the CA has been added trusted as root CA.

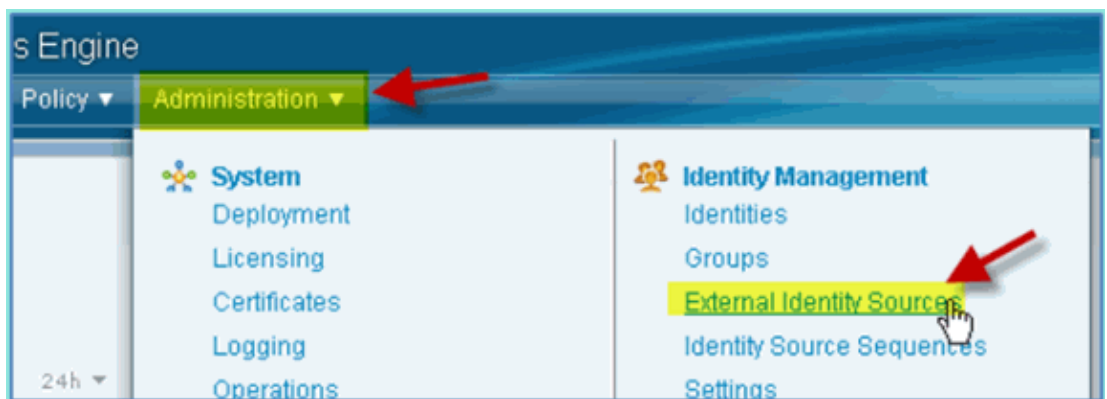


Windows 2008 Active Directory Integration

ISE can communicate directly with Active Directory (AD) for user/machine authentication or for retrieving authorization information user attributes. In order to communicate with AD, ISE must be joined to an AD domain. In this exercise you will join ISE to an AD domain, and confirm AD communication is working correctly.

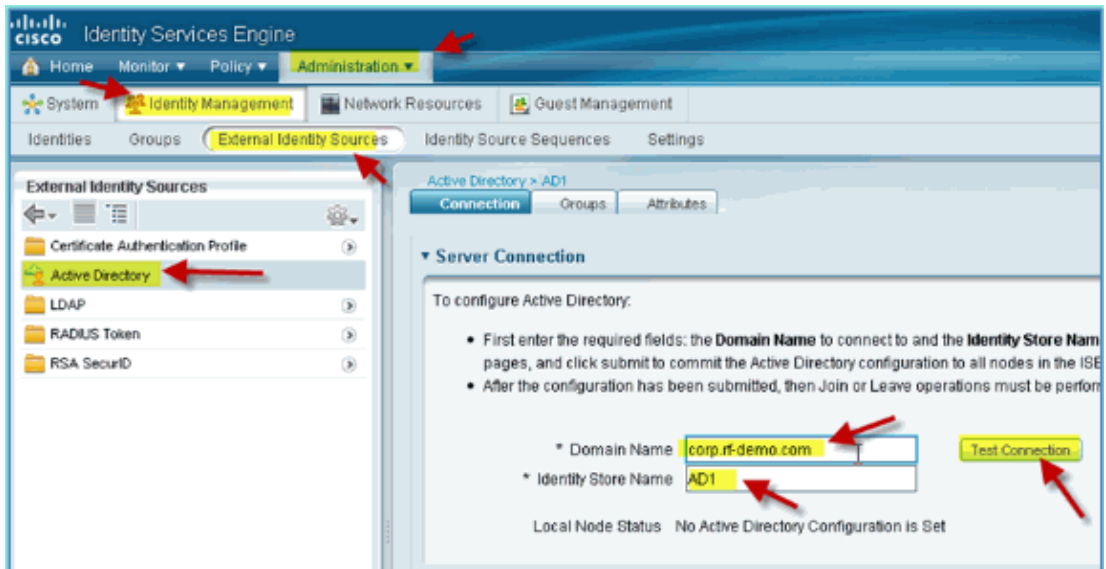
Complete these steps:

1. In order to join ISE to the AD domain, from ISE go to **Administration > Identity Management > External Identity Sources**.

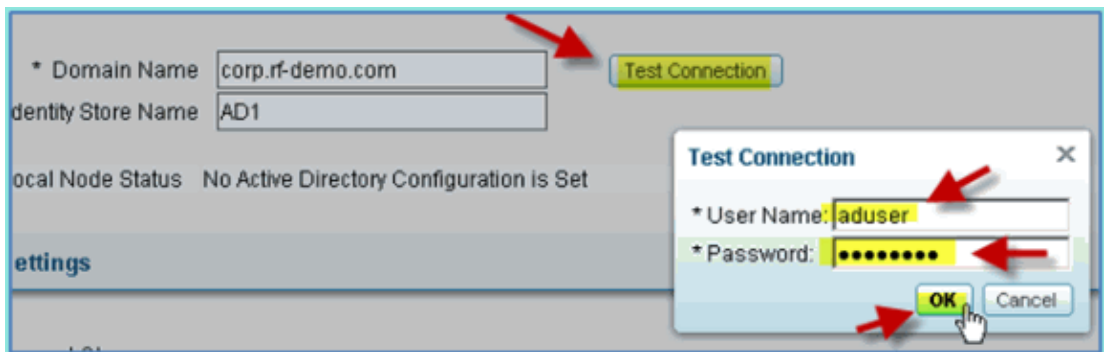


2. From the left pane (External Identity Sources), select **Active Directory**.
3. On the right-hand side, select the **Connection** tab and enter the following:

- ◆ Domain Name: corp.rf-demo.com
- ◆ Identity Store Name: AD1



4. Click **Test Connection**. Enter AD username (aduser/Cisco123), then click **OK**.



5. Confirm that the Test Status shows **Test Succeeded**.

6. Select Show Detailed Log and observe details useful for troubleshooting. Click **OK** to continue.



7. Click **Save Configuration**.

The screenshot shows a configuration window with the following elements:

- * Domain Name: corp.rf-demo.com
- * Identity Store Name: AD1
- Local Node Status: No Active Directory Configuration is Set
- Connection Settings section with three checked options:
 - Enable Password Change
 - Enable Machine Authentication
 - Enable Machine Access Restrictions
- Aging Time (hours): 6 (Valid Range 1 to 8760)
- Buttons at the bottom: Save Configuration (highlighted in green and pointed to by a red arrow), Join, and Delete Configuration.

8. Click **Join**. Enter the AD user (administrator/Cisco123), then click **OK**.

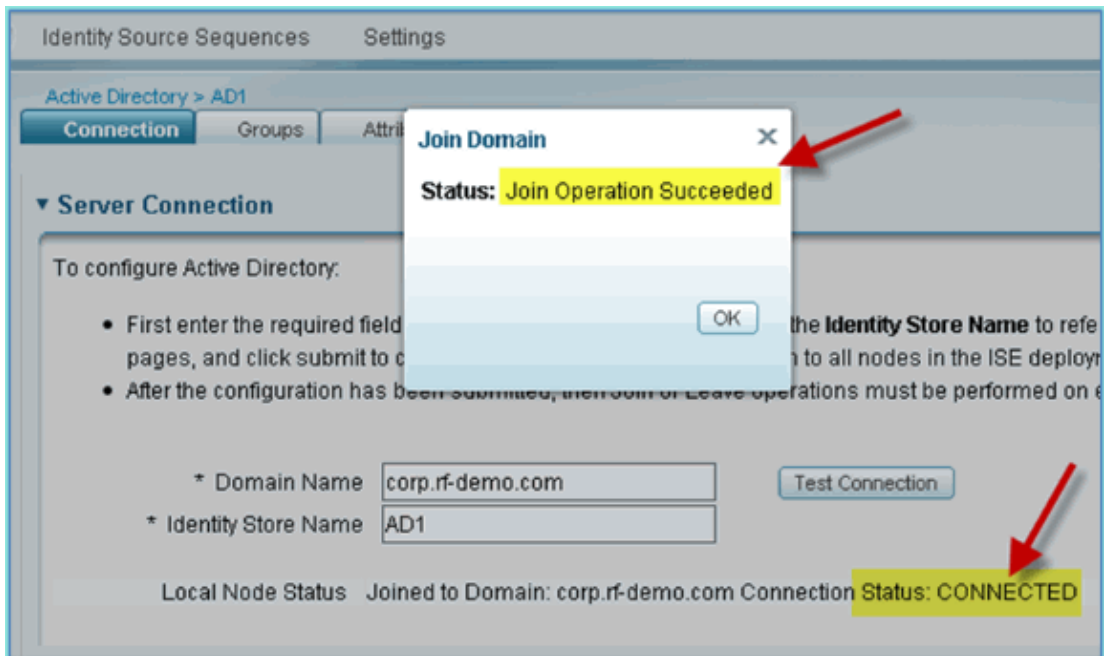
The screenshot shows the same configuration window as above, but with a 'Join Domain' dialog box open. The dialog box contains:

- * User Name: administrator (highlighted with a red arrow)
- * Password: [masked with dots] (highlighted with a red arrow)
- Buttons: OK (pointed to by a mouse cursor) and Cancel.

In the background configuration window, the 'Join' button is highlighted in green and pointed to by a red arrow. The 'Local Node Status' is now 'Not Joined to a domain'.

9. Confirm that Join Operation Status shows **Succeeded**, then click **OK** to continue.

The Server Connection Status shows **CONNECTED**. If this Status changes at any time, a Test Connection will help troubleshoot issues with the AD operations.



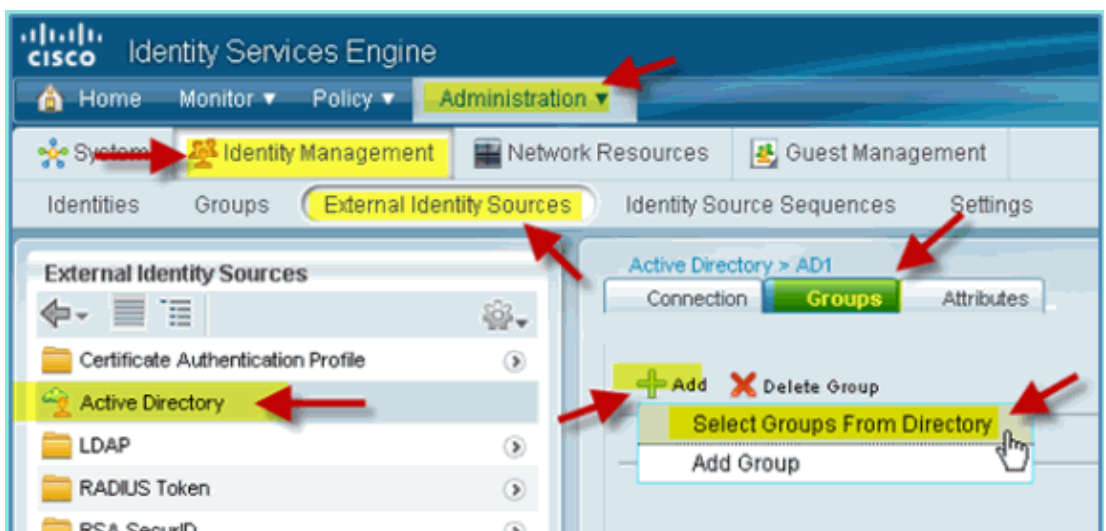
Add Active Directory Groups

When AD groups are added, more granular control is allowed over ISE policies. For example, AD groups can be differentiated by functional roles, such as Employee or Contractor groups, without the related bug being experienced in previous ISE 1.0 exercises where policies were limited only to users.

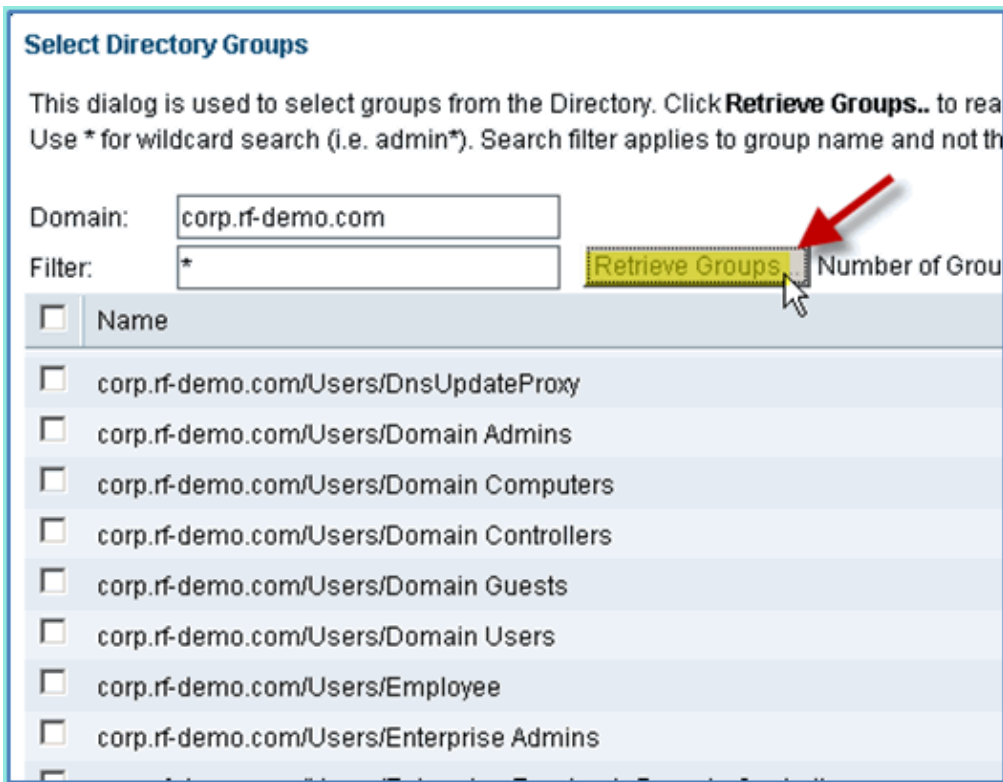
In this lab, only the Domain Users and/or the Employee group are used.

Complete these steps:

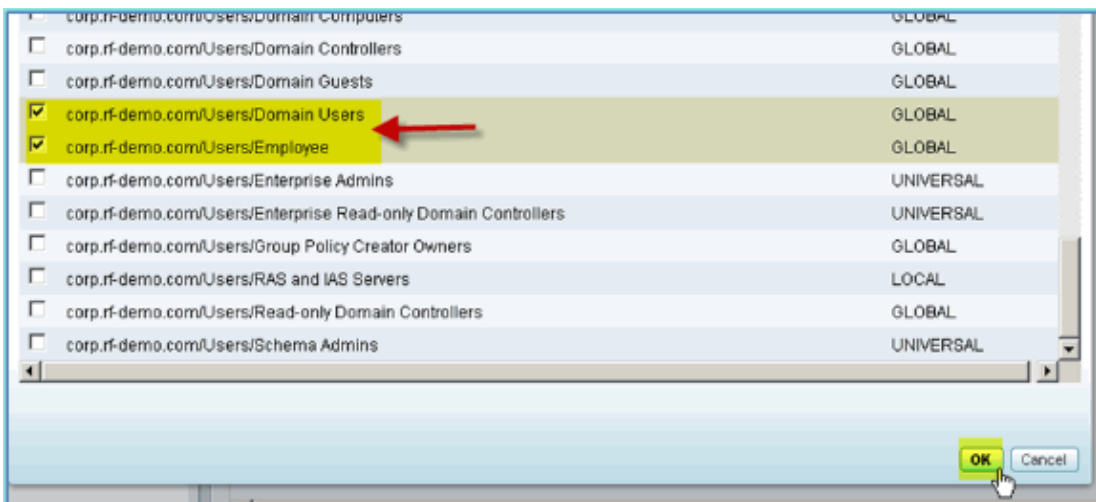
1. From ISE, go to **Administration > Identity Management > External Identity Sources**.
2. Select **Active Directory > Groups** tab.
3. Click **+Add**, then **Select Groups From Directory**.



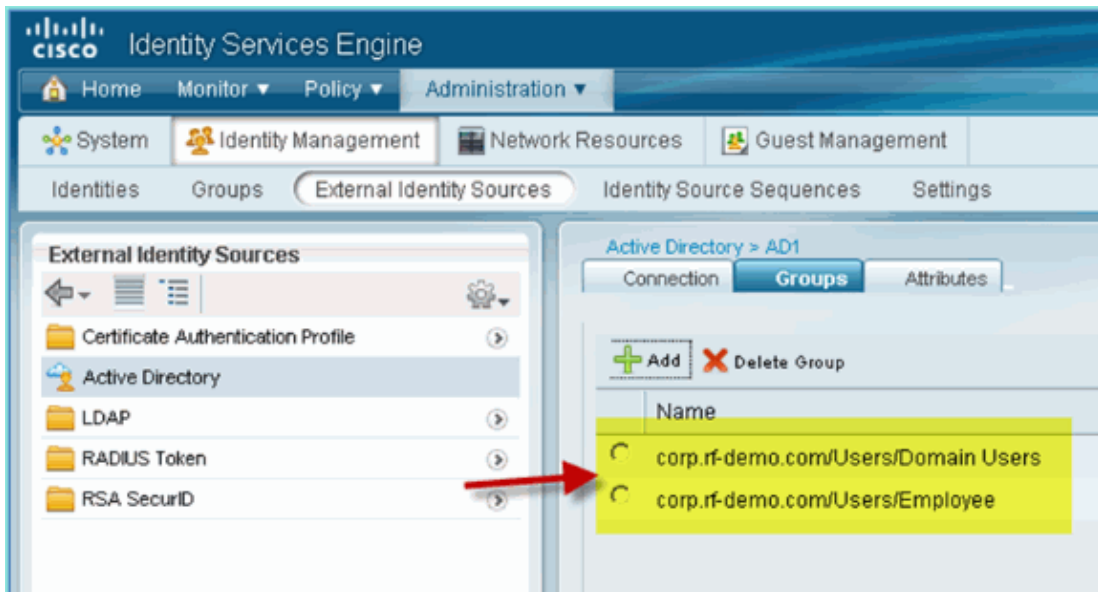
4. In the follow-up window (Select Directory Groups), accept the defaults for domain (corp-rf-demo.com) and Filter (*). Then, click **Retrieve Groups**.



5. Select the boxes for **Domain Users** and **Employee** groups. Click **OK** when finished.



6. Confirm that the groups have been added to the list.

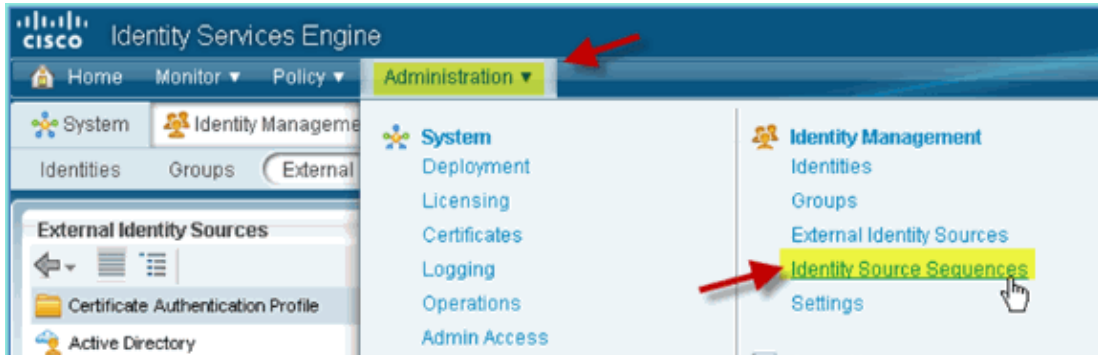


Add Identity Source Sequence

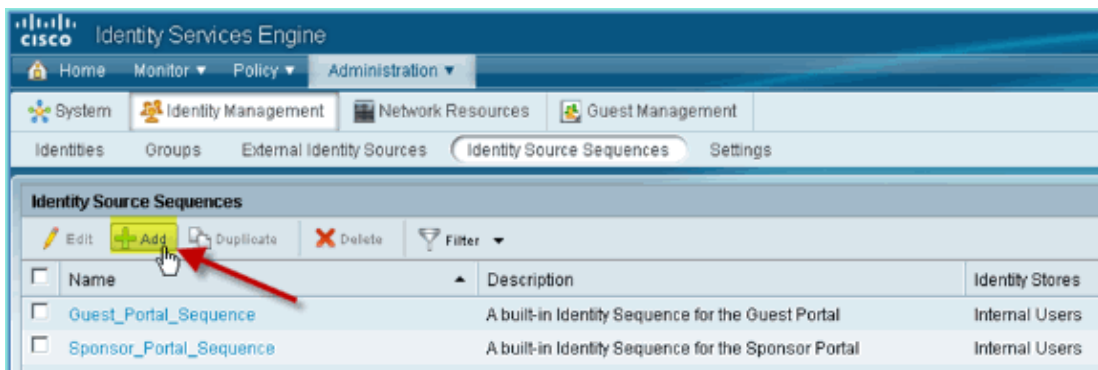
By default, ISE is set to use Internal Users for authentication store. If AD is added, a priority order of sequence can be created to include the AD which ISE will use to check for authentication.

Complete these steps:

1. From ISE, navigate to **Administration > Identity Management > Identity Source Sequences**.



2. Click **+Add** in order to add a new sequence.



3. Enter the new name: **AD_Internal**. Add all available sources to the Selected field. Then, re-order as needed so that AD1 is moved to the top of the list. Click **Submit**.

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Source Sequences List > New Identity Source Sequence

Identity Source Sequence

* Name

Description

Certificate Based Authentication

Select Certificate Authentication Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
	AD1 Internal Users Internal Endpoints

Advanced Search List Settings

Select the action to be performed if a selected identity store cannot be accessed for authentication

Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

Treat as if the user was not found and proceed to the next store in the sequence

4. Confirm that the sequence has been added to the list.

Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Source Sequences

Edit Add Duplicates Delete Filter

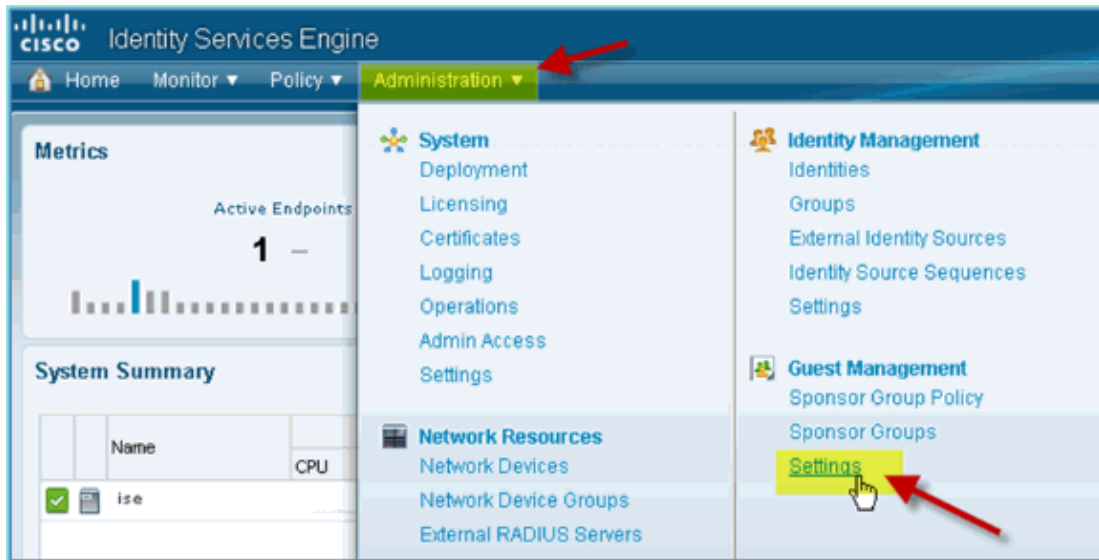
Name	Description	Identity Stores
AD_Internal		AD1,Internal Endpoints,Internal Users
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

ISE Wireless Sponsored Guest Access with Integrated AD

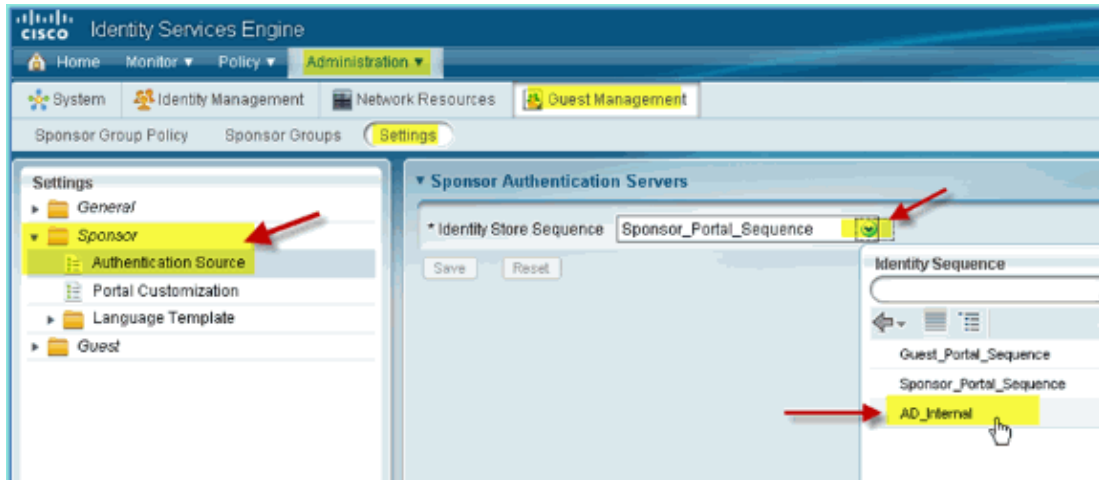
ISE can be configured to allow guests to be sponsored with policies in order to allow AD domain users to sponsor guest access.

Complete these steps:

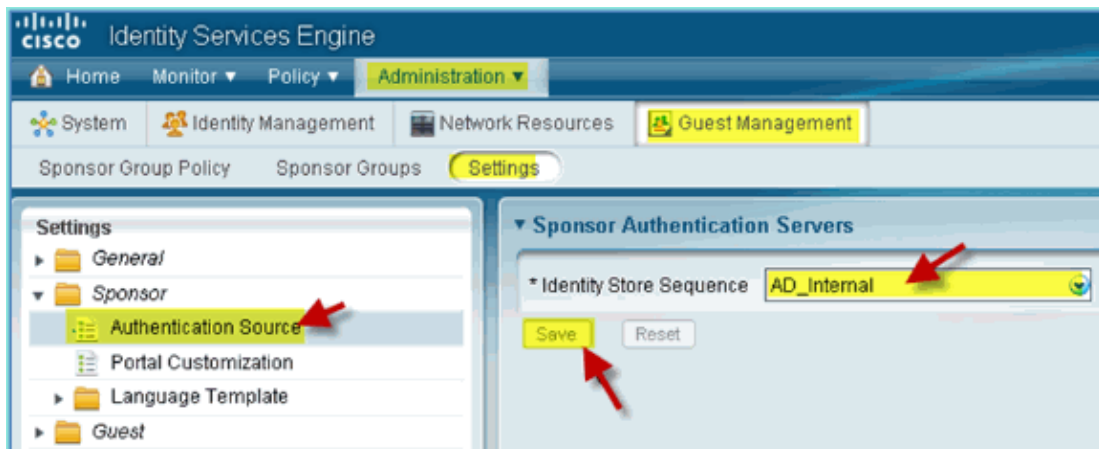
1. From ISE, navigate to **Administration > Guest Management > Settings**.



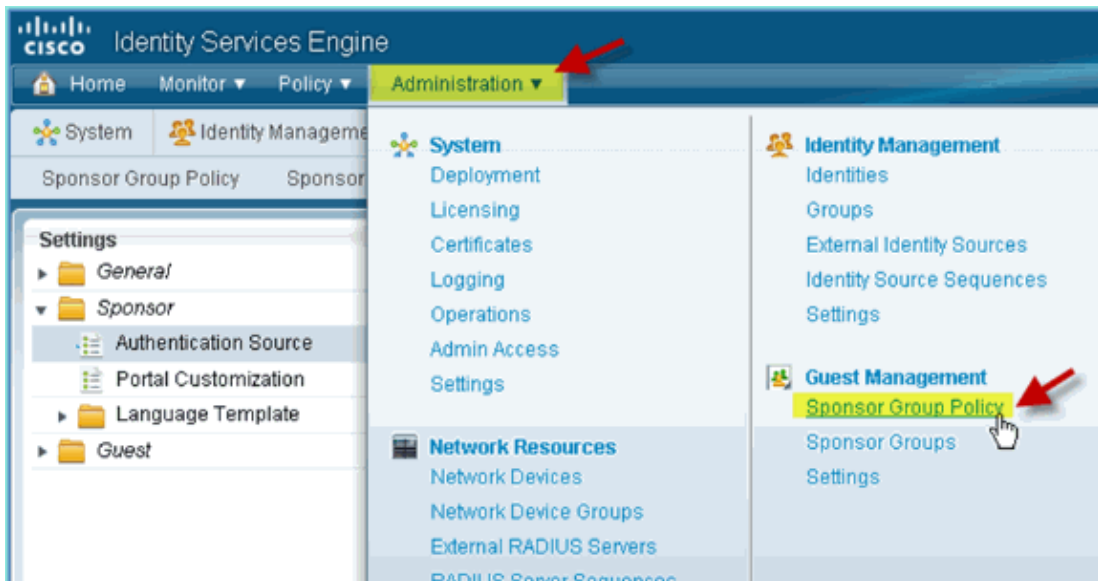
2. Expand **Sponsor**, and click **Authentication Source**. Then, select **AD_Internal** as Identity Store Sequence.



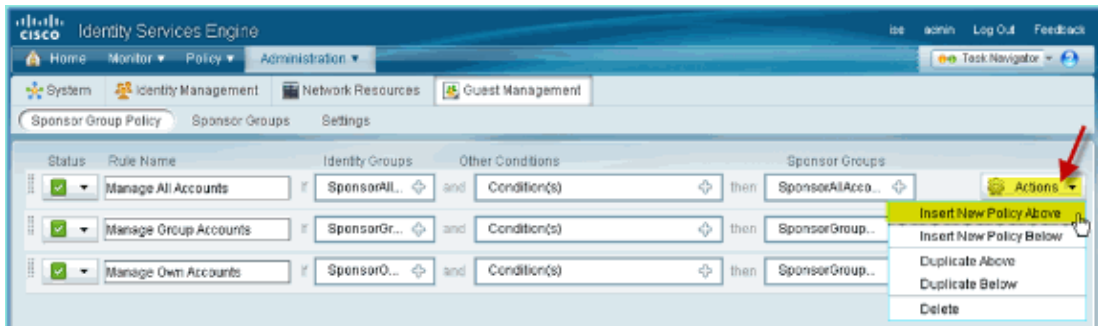
3. Confirm **AD_Internal** as the Identity Store Sequence. Click **Save**.



4. Navigate to **Administration > Guest Management > Sponsor Group Policy**.

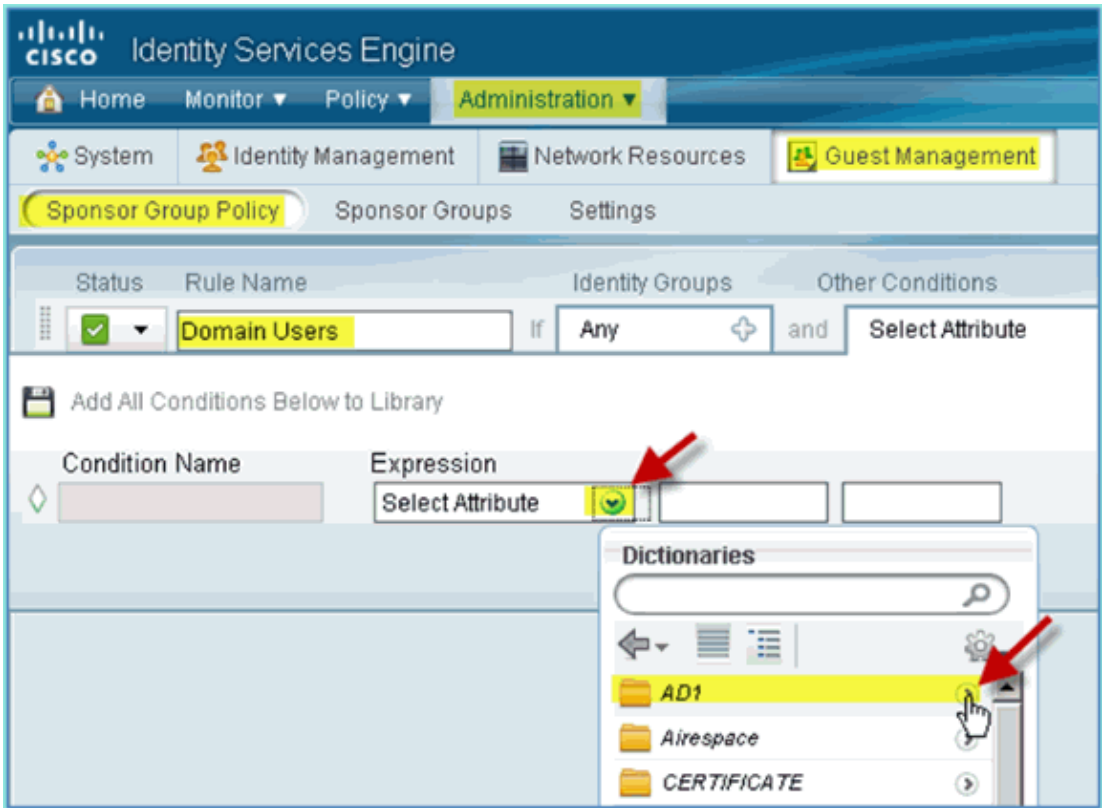


5. Insert New Policy Above the first rule (click the **Actions** icon from the right).

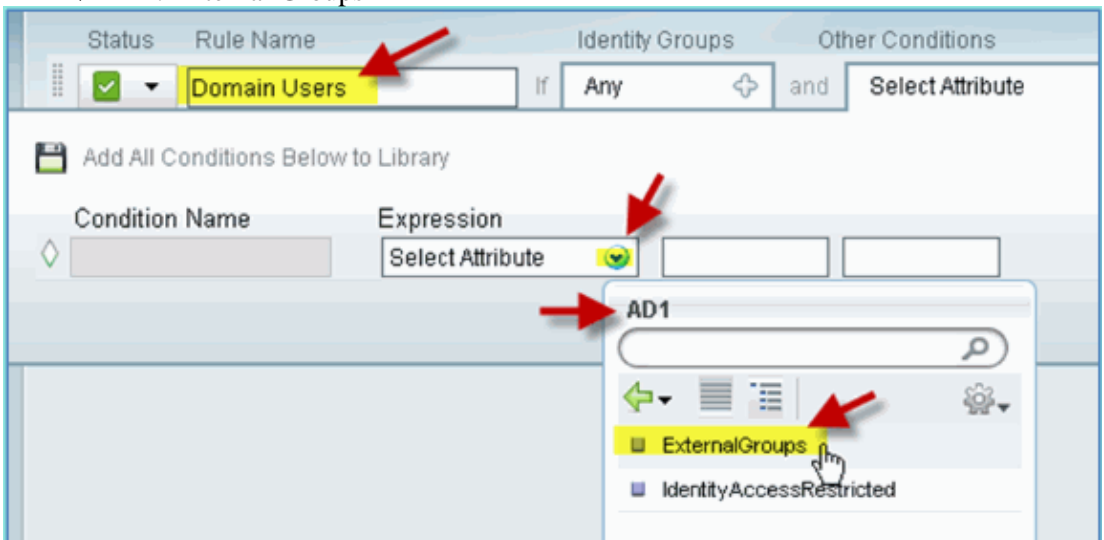


6. For the new Sponsor Group Policy, create the following:

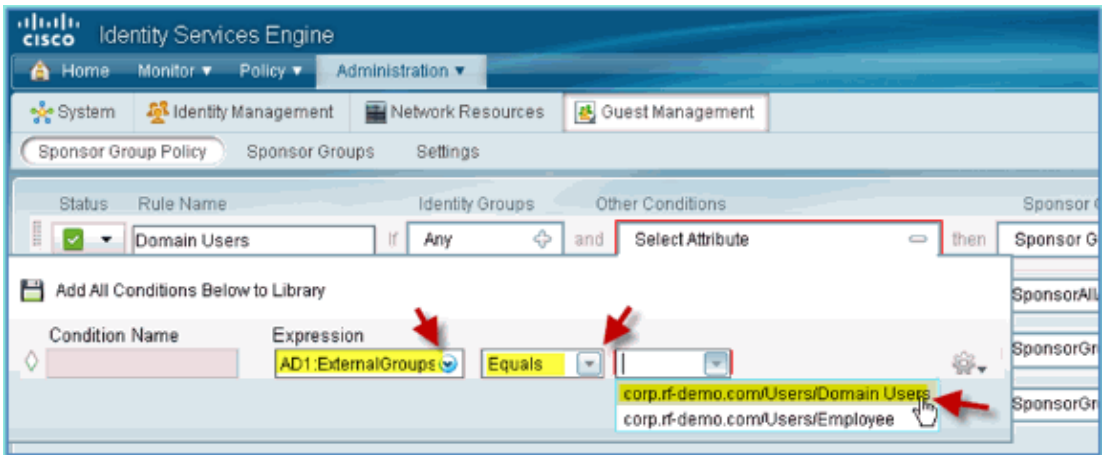
- ◆ Rule Name: Domain Users
- ◆ Identity Groups: Any
- ◆ Other Conditions: (Create New / Advanced) > AD1



◆ AD1: External Groups

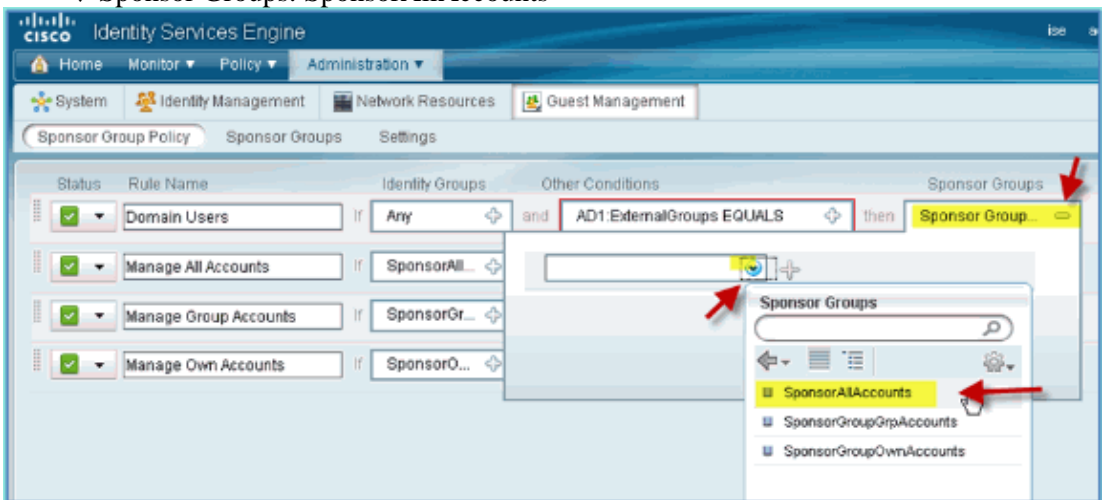


◆ AD1 External Groups > Equals > corp.rf-demo.com/Users/Domain Users

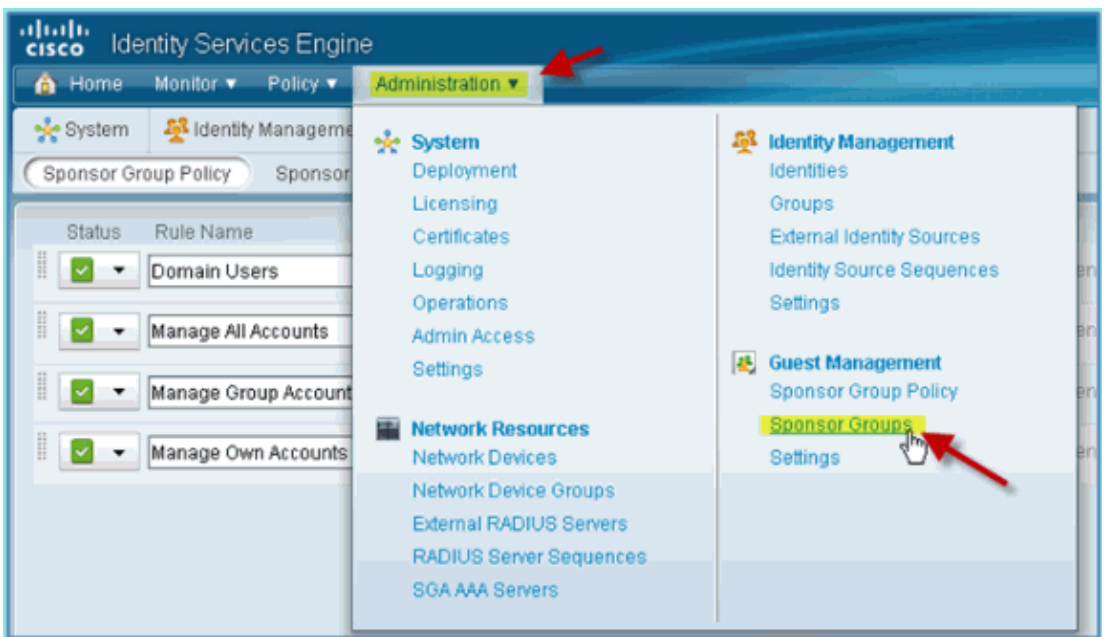


7. In Sponsor Groups, set the following:

◆ Sponsor Groups: SponsorAllAccounts



8. Navigate to **Administration > Guest Management > Sponsor Groups**.



9. Select to Edit > **SponsorAllAccounts**.

Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Sponsor Group Policy Sponsor Groups Settings

Guest Sponsor Groups

Edit Add Delete Filter

<input type="checkbox"/>	Sponsor Group Name	Description
<input checked="" type="checkbox"/>	SponsorAllAccounts	Default SponsorGroup
<input type="checkbox"/>	SponsorGroupGrpAccounts	Default SponsorGroup

10. Select Authorization Levels and set the following:

- ◆ View Guest Password: Yes

Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Sponsor Group Policy Sponsor Groups Settings

Sponsor Group List > SponsorAllAccounts

General **Authorization Levels** Guest Roles Time Profiles

Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	No
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	1 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)

Save Reset

Configure SPAN on the Switch

Configure SPAN – ISE mgt/probe interface is L2 adjacent to WLC management interface. The switch can be configured to SPAN and other interfaces, such as employee and guest interface VLANs.

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
```

ISE virtual probe interface.

Reference : Wireless Authentication for Apple MAC OS X

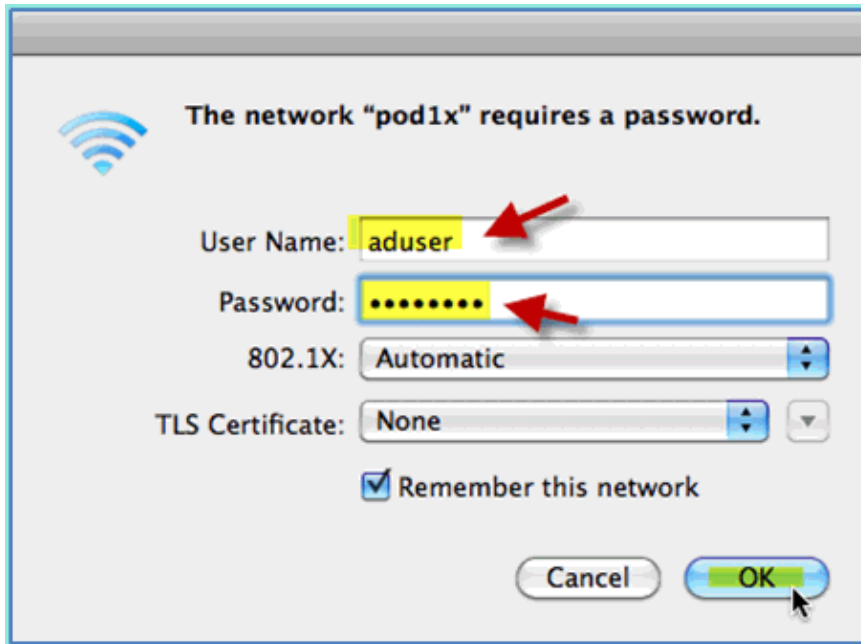
Associate to the WLC via an authenticated SSID as an INTERNAL user (or integrated, AD User) using an Apple Mac OS X wireless laptop. Skip if not applicable.

1. On a Mac, go to the WLAN settings. Enable WIFI, then select and connect to the 802.1X enabled POD SSID created in the previous exercise.



2. Provide the following information to connect:

- ◆ Username: aduser (if using AD), employee (internal Employee), contractor (internal Contractor)
- ◆ Password: XXXX
- ◆ 802.1X: Automatic
- ◆ TLS Certificate: None

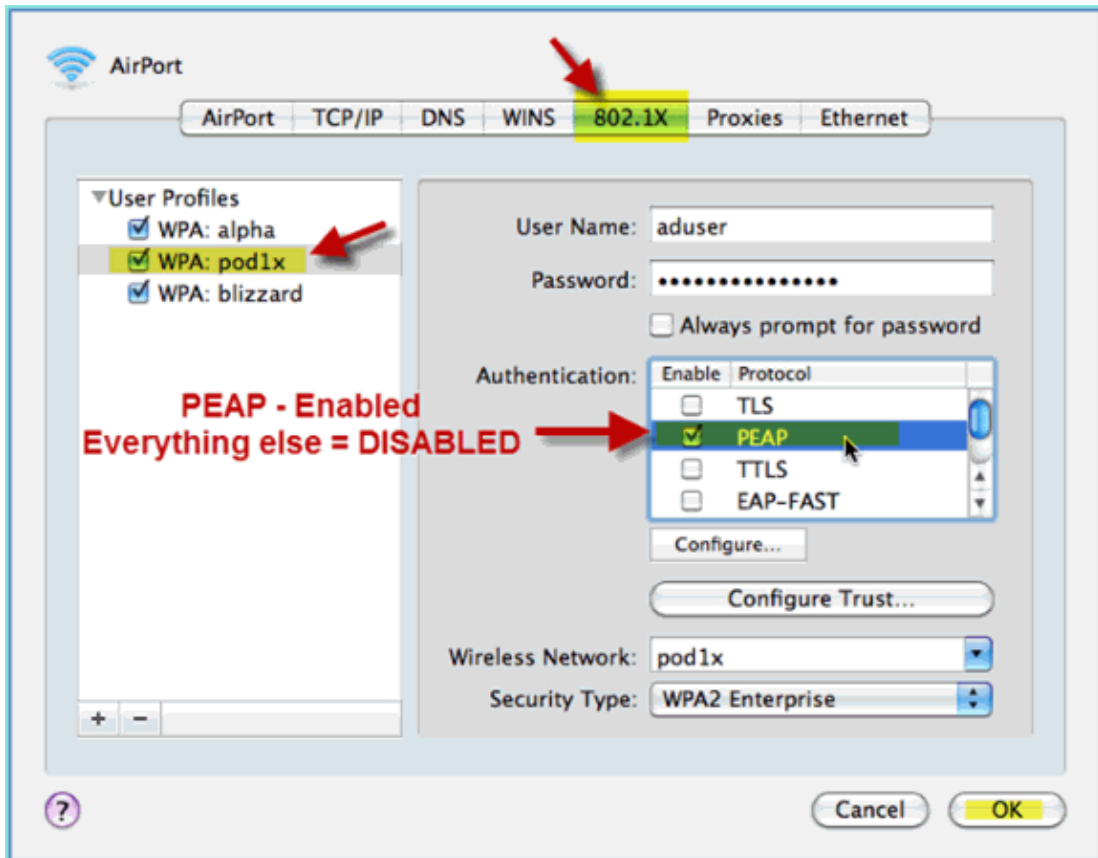


At this time, the laptop might not connect. In addition, ISE can throw a failed event as follows:

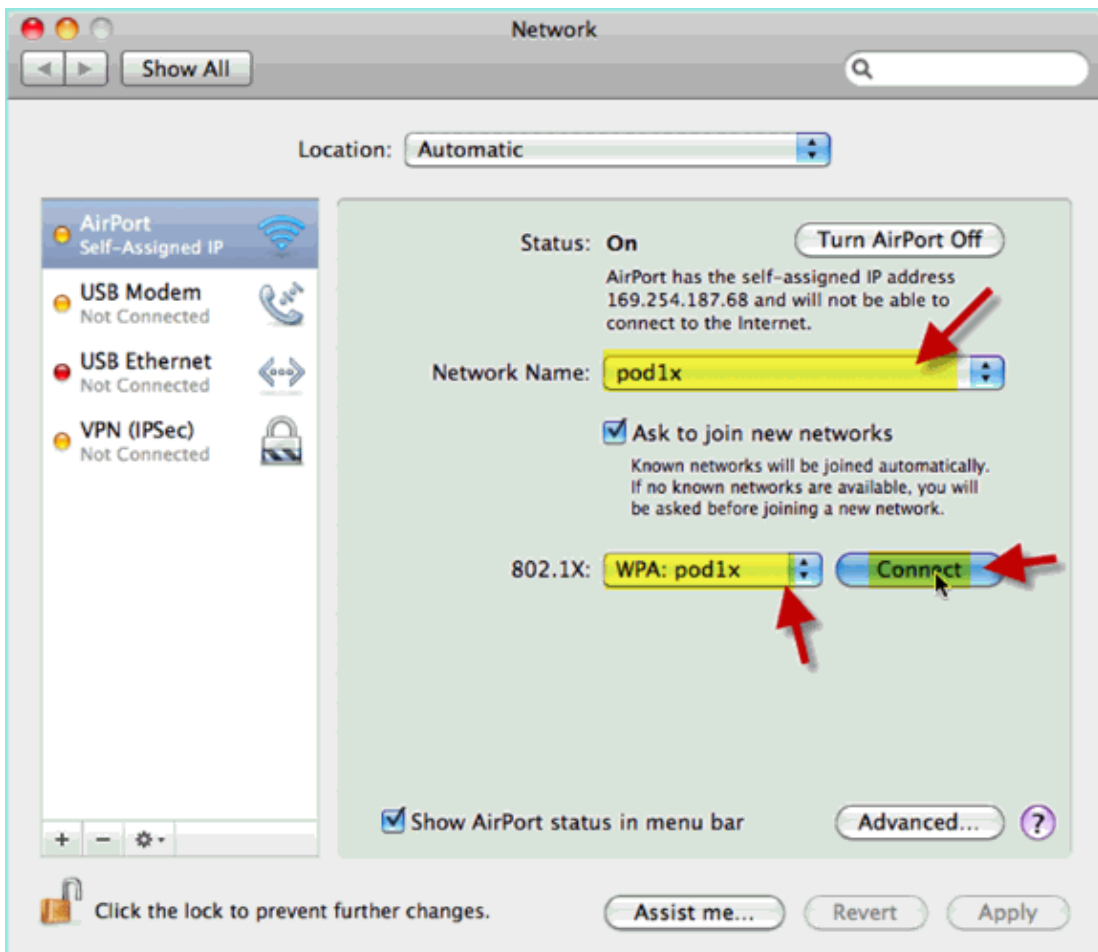
```
Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of  
an unknown CA in the client certificates chain
```

3. Go to the **System Preference > Network > Airport > 802.1X** setting and set the new POD SSID/WPA profile Authentication as:

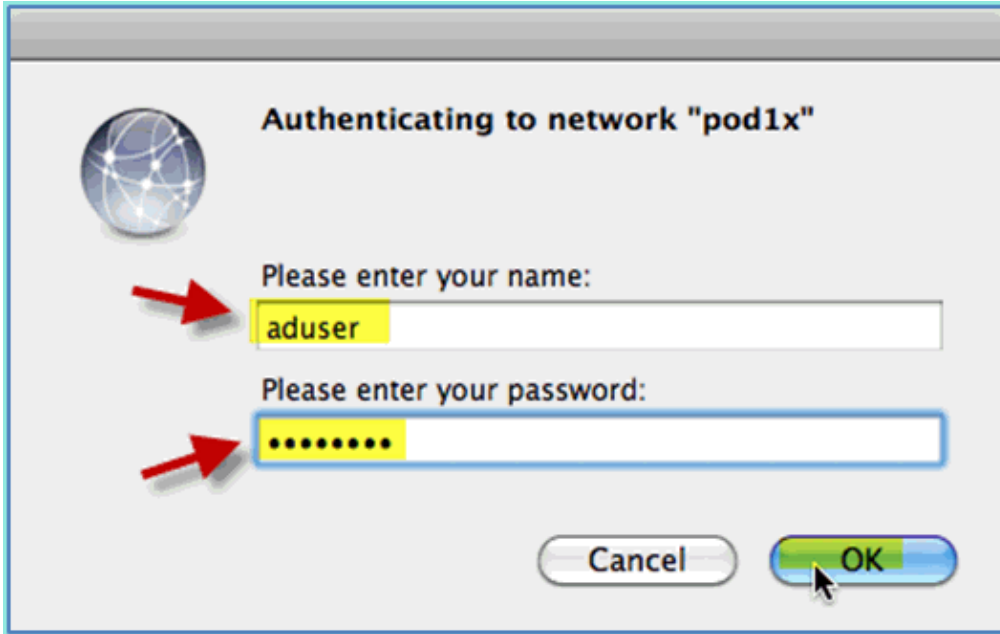
- ◆ TLS: Disabled
- ◆ PEAP: Enabled
- ◆ TTLS: Disabled
- ◆ EAP-FAST: Disabled



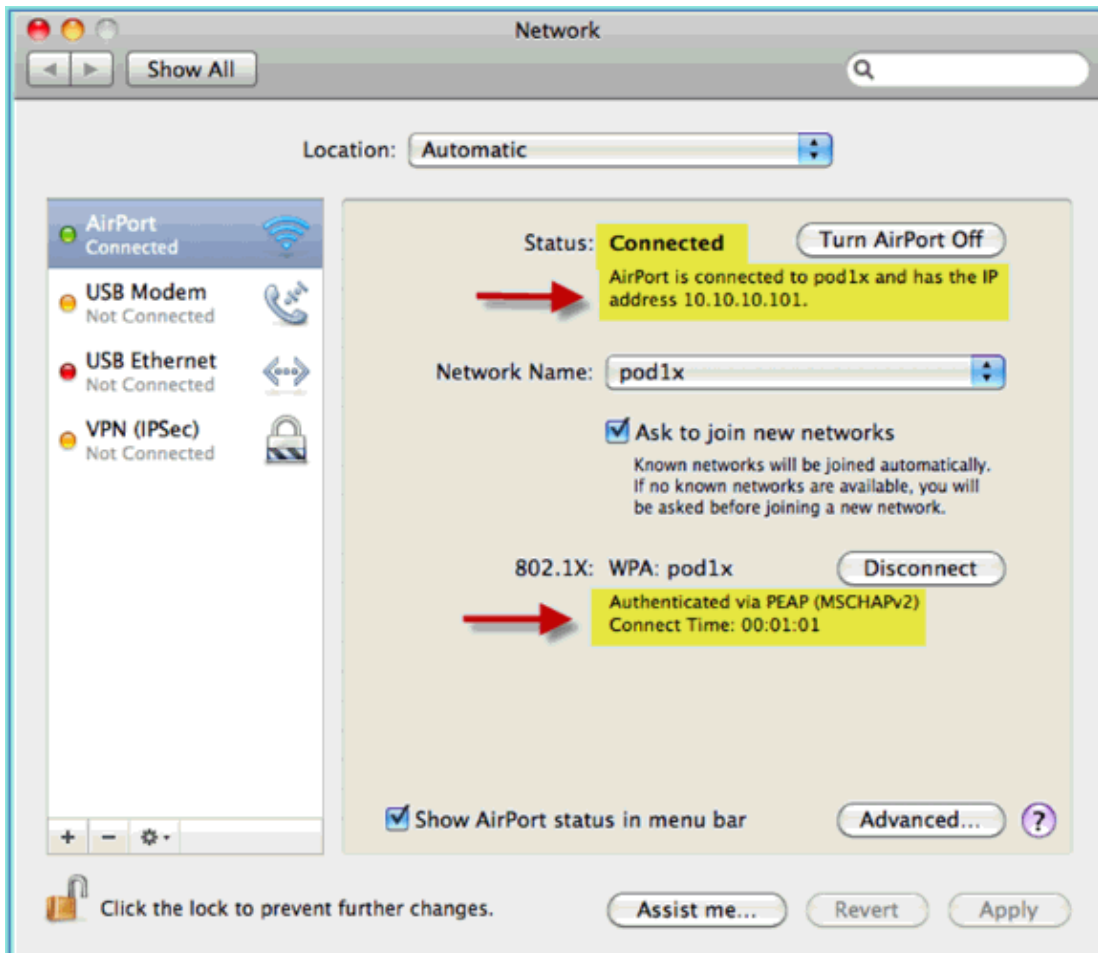
4. Click **OK** to continue and allow the setting to be saved.
5. On the Network screen, select the appropriate SSID + 802.1X WPA profile and click **Connect**.



6. The System might prompt for a username and password. Enter the AD user and password (aduser/XXXX), then click **OK**.



The client should show **Connected** via PEAP with a valid IP address.

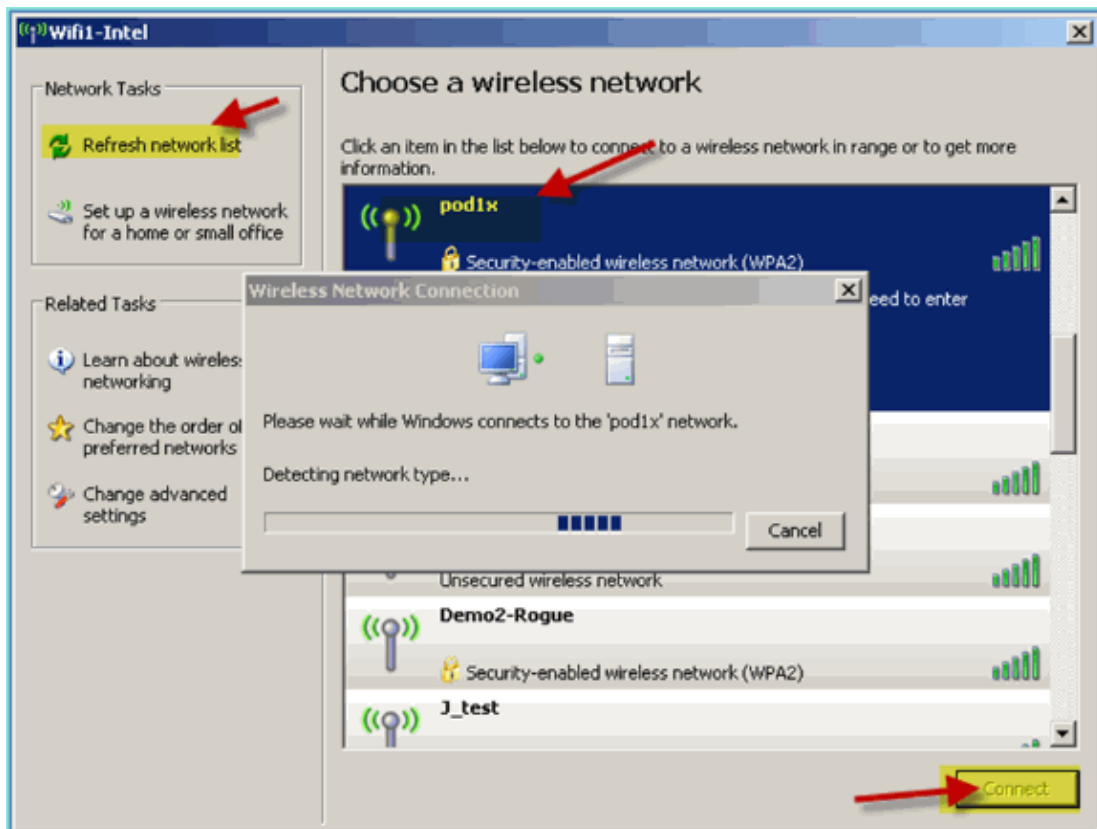


Reference : Wireless Authentication for Microsoft Windows XP

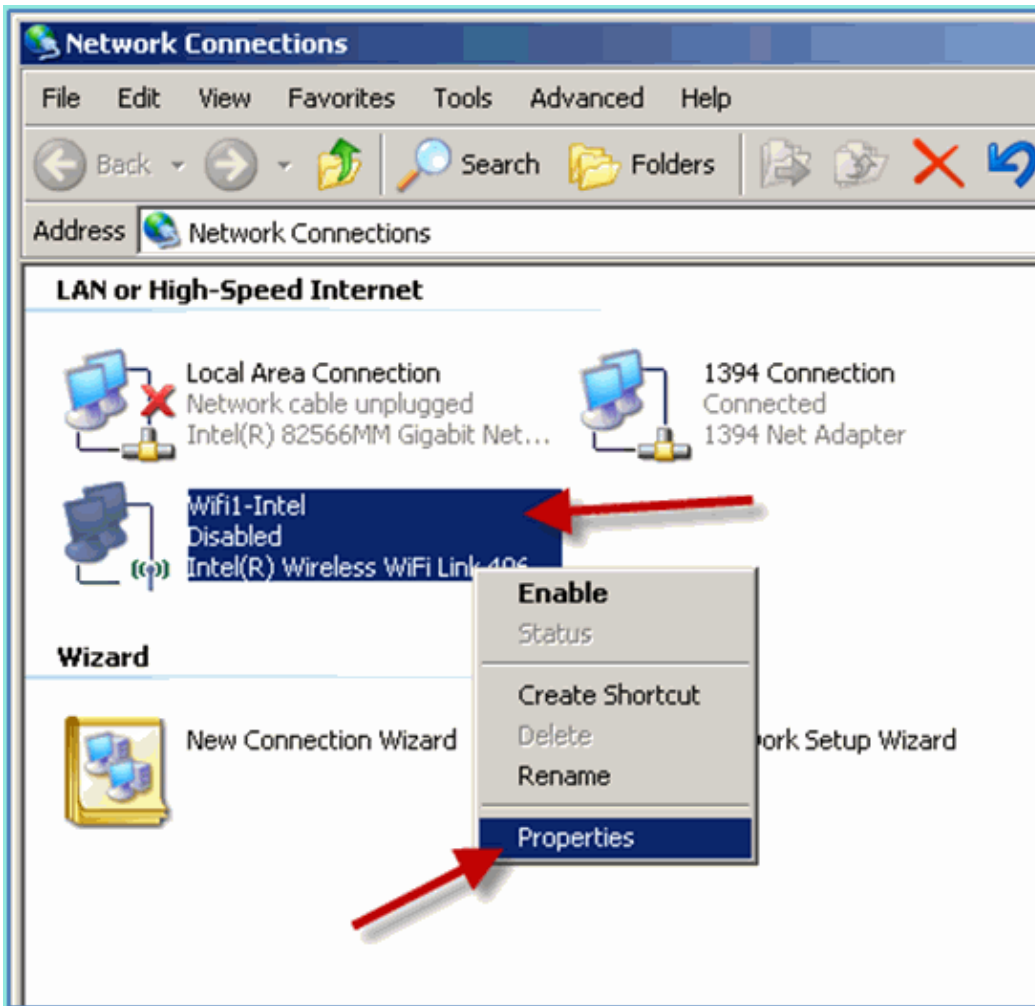
Associate to the WLC via an authenticated SSID as an INTERNAL user (or integrated, AD User) using a Windows XP wireless laptop. Skip if not applicable.

Complete these steps:

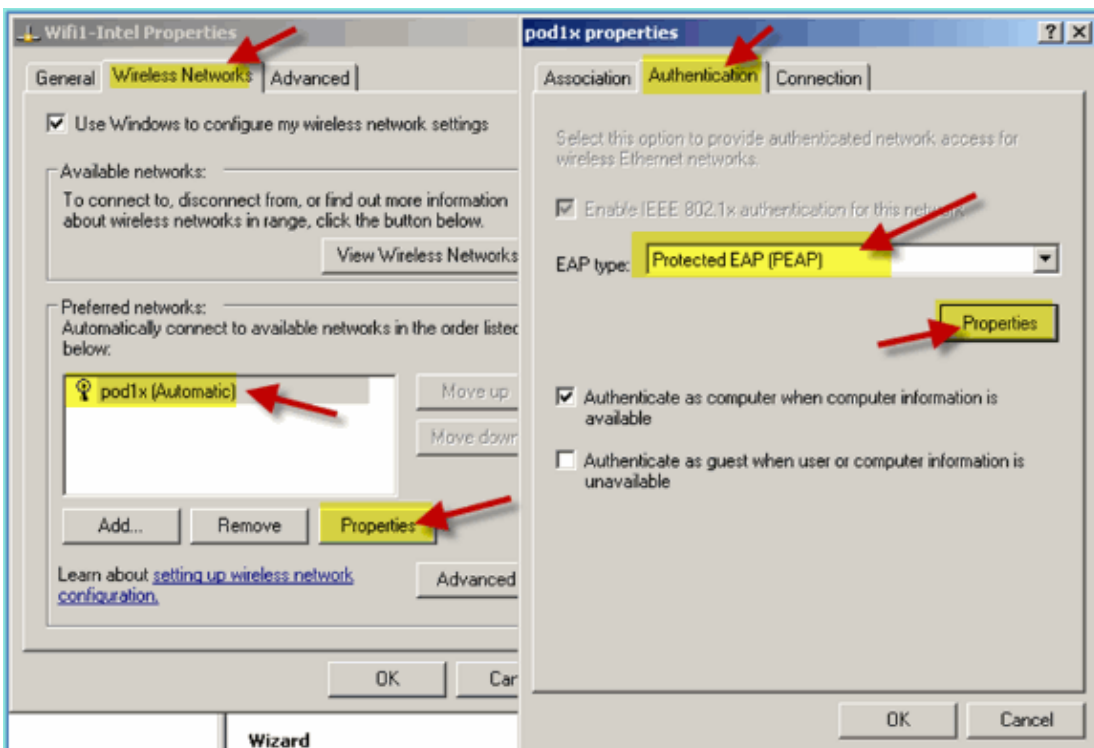
1. On the laptop, go to the WLAN settings. Enable WIFI and connect to the 802.1X enabled POD SSID created in the previous exercise.



2. Access the network properties for the WIFI interface.



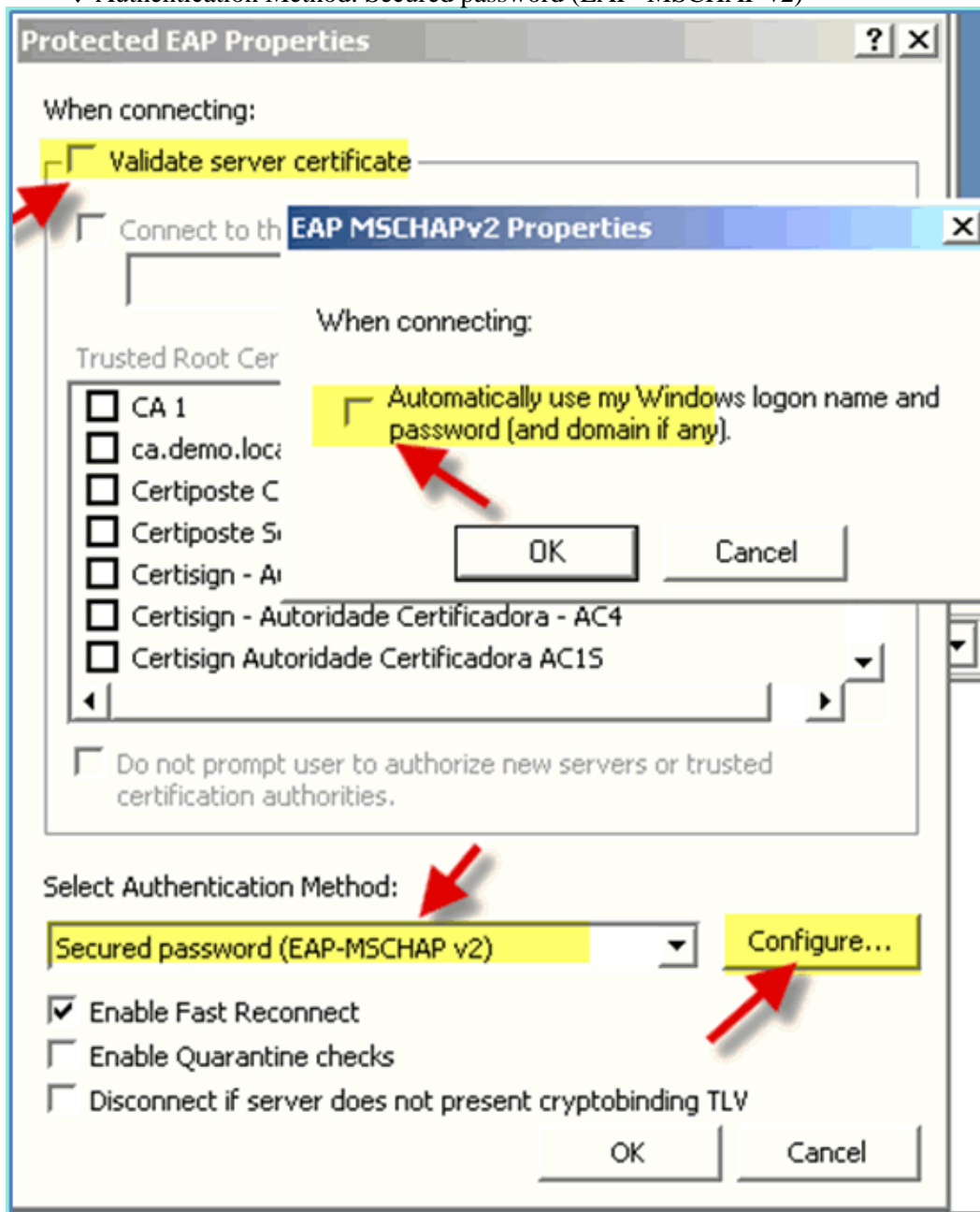
3. Navigate to the **Wireless Networks** tab. Select the pod SSID network properties > Authentication tab > EAP type = Protected EAP (PEAP).



4. Click the EAP Properties.

5. Set the following:

- ◆ Validate server certificate: Disabled
- ◆ Authentication Method: Secured password (EAP-MSCHAP v2)



6. Click **OK** on all windows to complete this configuration task.

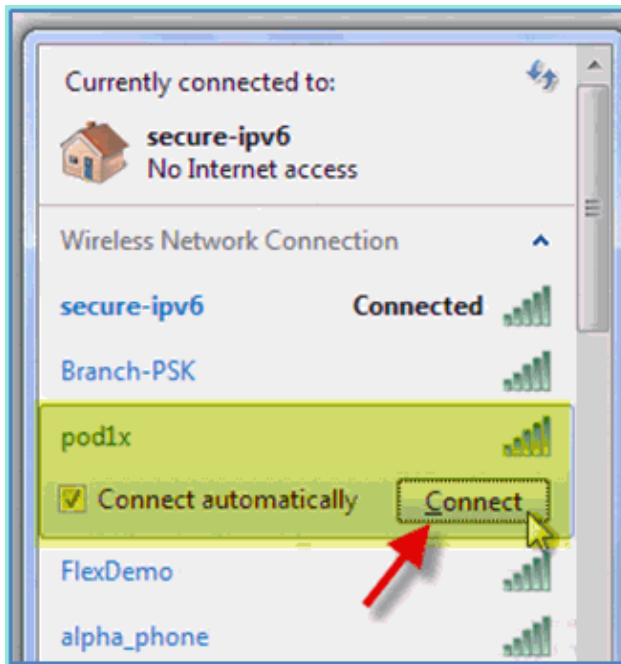
7. Windows XP client prompts for the username and password. In this example, it is aduser/XXXX.

8. Confirm network connectivity, IP addressing (v4).

Reference: Wireless Authentication for Microsoft Windows 7

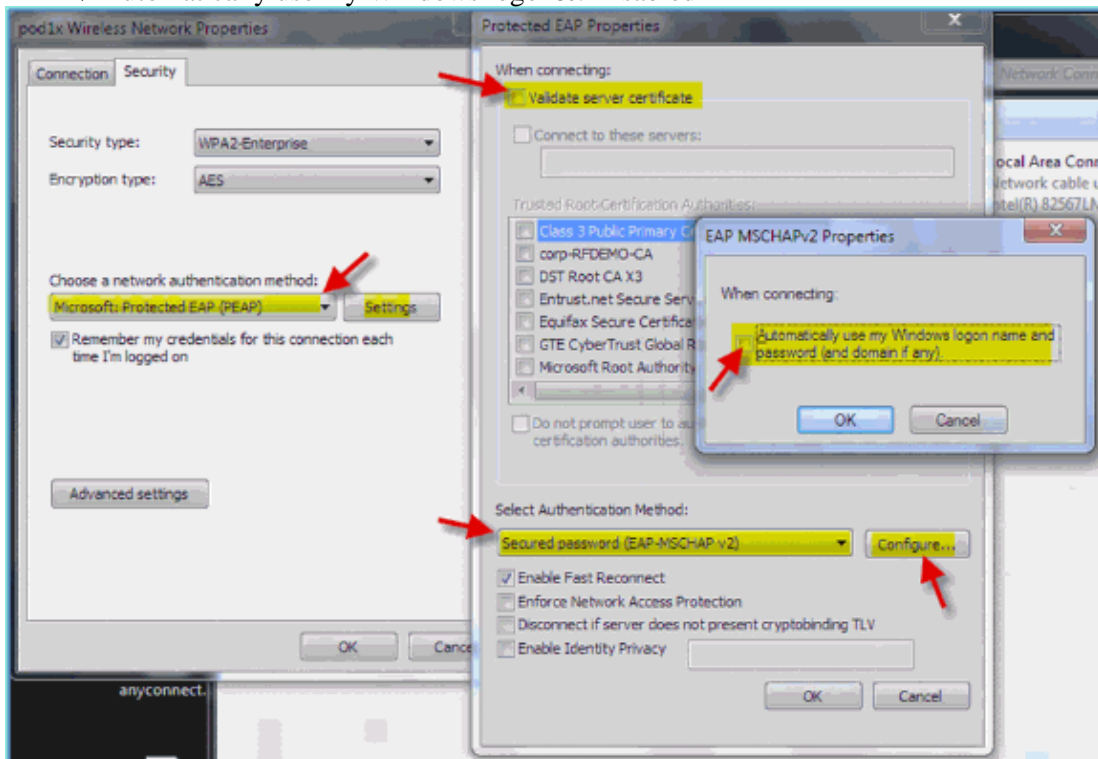
Associate to the WLC via an authenticated SSID as an INTERNAL user (or integrated, AD User) using a Windows 7 wireless laptop.

1. On the laptop, go to the WLAN settings. Enable WIFI and connect to the 802.1X enabled POD SSID created in the previous exercise.



2. Access the Wireless Manager and edit the new POD wireless profile.
3. Set the following:

- ◆ Authentication Method: PEAP
- ◆ Remember my credentials&: Disabled
- ◆ Validate server certificate (advanced setting): Disabled
- ◆ Authentication Method (adv. Setting): EAP-MSCHAP v2
- ◆ Automatically use my Windows logon&: Disabled



Related Information

- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Apr 09, 2012

Document ID: 113476
