Wireless BYOD for FlexConnect Deployment Guide

Document ID: 113606

Contributed by Surendra BG and Ramamurthy Bakthavatchalam, Cisco TAC Engineers.

Sep 12, 2013

Contents

Introduction
Prerequisites
- Requirements
- Components Used
- Topology

Device Registration and Supplicant Provisioning
Asset Registration Portal
Self−Registration Portal
Authentication and Provisioning
Provisioning for iOS (iPhone/iPad/iPod)
Provisioning for Android
Dual SSID Wireless BYOD Self−Registration
Single SSID Wireless BYOD Self−Registration
Feature Configuration
- WLAN Configuration
- FlexConnect AP Configuration
- ISE Configuration

User Experience − Provisioning iOS
- Dual SSID
- Single SSID

User Experience − Provisioning Android
- Dual SSID

My Devices Portal
Reference − Certificates
Related Information

Introduction

Mobile devices are becoming more computationally powerful and popular among consumers. Millions of these devices are sold to consumers with high−speed Wi−Fi so users can communicate and collaborate. Consumers are now accustomed to the productivity enhancement these mobile devices bring into their lives and are seeking to bring their personal experience into the workspace. This creates the functionality needs of a Bring Your Own Device (BYOD) solution in the workplace.

This document provides the branch deployment for the BYOD solution. An employee connects to a corporate service set identifier (SSID) with his/her new iPad and gets redirected to a self−registration portal. The Cisco Identity Services Engine (ISE) authenticates the user against the corporate Active Directory (AD) and downloads a certificate with an embedded iPad MAC address and username to the iPad, along with a supplicant profile that enforces the use of the Extensible Authentication Protocol−Transport Layer Security (EAP−TLS) as a method for dot1x connectivity. Based on the authorization policy in ISE, the user can then

connect with the use of dot1x and gain access to appropriate resources.

ISE functionalities in Cisco Wireless LAN Controller software releases earlier than 7.2.110.0 did not support local switching clients that associate through FlexConnect access points (APs). Release 7.2.110.0 supports these ISE functionalities for FlexConnect APs for local switching and centrally authenticated clients. Furthermore, Release 7.2.110.0 integrated with ISE 1.1.1 provides (but is not limited to) these BYOD solution features for wireless:

- Device profiling and posture
- Device registration and supplicant provisioning
- Onboarding of personal devices (provision iOS or Android devices)

Note: Although supported, other devices, such as PC or Mac wireless laptops and workstations, are not included in this guide.

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:

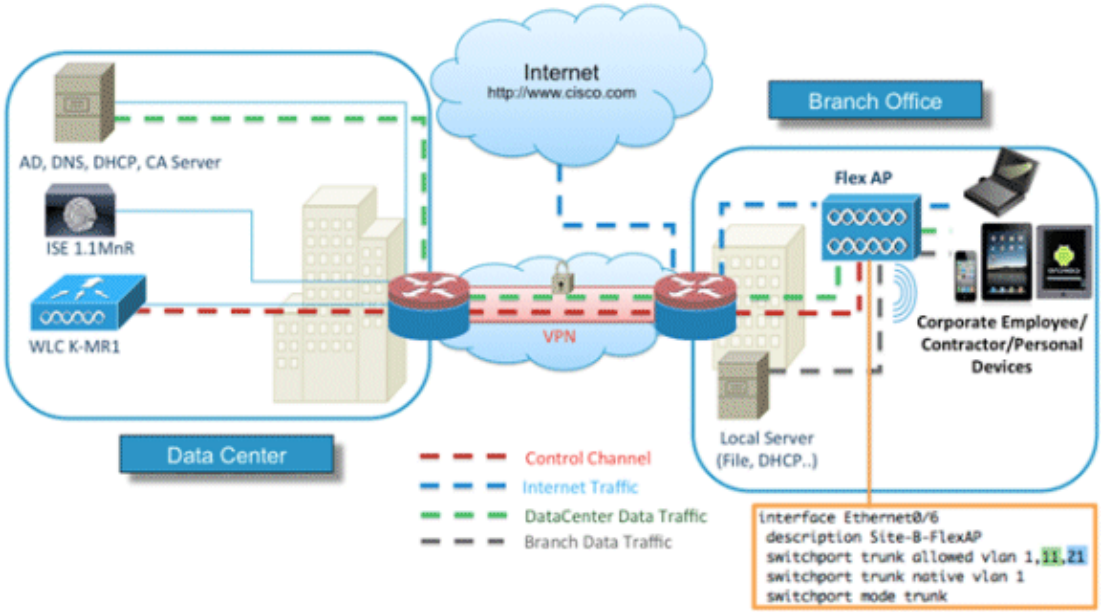
- Cisco Catalyst Switchs
- Cisco Wireless LAN (WLAN) Controllers
- Cisco WLAN Controller (WLC) Software Release 7.2.110.0 and later
- 802.11n APs in FlexConnect mode
- Cisco ISE Software Release 1.1.1 and later
- Windows 2008 AD with Certificate Authority (CA)
- DHCP server
- Domain Name System (DNS) server
- Network Time Protocol (NTP)
- Wireless client laptop, smartphone, and tablets (Apple iOS, Android, Windows, and Mac)

Note: Refer to Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.2.110.0 for important information about this software release. Log in to the Cisco.com site for the latest release notes before you load and test software.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Topology

A minimal network setup, as shown in this diagram is required in order to properly implement and test these features:



For this simulation, you need a network with a FlexConnect AP, a local/remote site with local DHCP, DNS, the WLC, and the ISE. The FlexConnect AP is connected to a trunk in order to test local switching with multiple VLANs.

Device Registration and Supplicant Provisioning

A device must be registered so that its native supplicant can provisioned for dot1x authentication. Based on the right authentication policy, the user is redirected to the guest page and authenticated by employee credentials. The user sees the device registration page, which asks for their device information. The device provisioning process then begins. If the operating system (OS) is not supported for provisioning, the user is redirected to the Asset Registration Portal in order to mark that device for MAC Authentication Bypass (MAB) access. If the OS is supported, the enrollment process begins and configures the native supplicant of the device for dot1x authentication.

Asset Registration Portal

The Asset Registration Portal is the element of the ISE platform that allows employees to initiate the onboarding of endpoints through an authentication and registration process.

Administrators are able to delete assets from the endpoints identities page. Each employee is able to edit, delete, and blacklist the assets they have registered. Blacklisted endpoints are assigned to a blacklist identity group, and an authorization policy is created in order to prevent network access by blacklisted endpoints.

Self−Registration Portal

In the Central Web Authentication (CWA) flow, employees are redirected to a portal that allows them to enter their credentials, authenticate, and enter the specifics of the particular asset they wish to register. This portal is called the Self Provisioning Portal and is similar to the Device Registration Portal. It allows the employees to enter the MAC address as well as a meaningful escription of the endpoint.

Authentication and Provisioning

Once employees select the Self−Registration Portal, they are challenged to provide a set of valid employee

credentials in order to proceed to the provisioning phase. After successful authentication, the endpoint can be provisioned into the endpoints database, and a certificate is generated for the endpoint. A link on the page allows the employee to download the Supplicant Pilot Wizard (SPW).

Note: Refer to the FlexConnect Feature Matrix Cisco article in order to view the latest FlexConnect feature matrix for BYOD.

Provisioning for iOS (iPhone/iPad/iPod)

For EAP−TLS configuration, ISE follows the Apple Over−the−Air (OTA) enrollment process:

- After successful authentication, the evaluation engine evaluates client−provisioning policies, which results in a supplicant profile.
- If the supplicant profile is for the EAP−TLS setting, the OTA process determines whether the ISE is using self−signed or signed by an unknown CA. If one of the conditions is true, the user is asked to download the certificate of either ISE or CA before the enrollment process can begin.
- For other EAP methods, ISE pushes the final profile upon successful authentication.

Provisioning for Android

Because of security considerations, the Android agent must be downloaded from the Android marketplace site and cannot be provisioned from ISE. Cisco uploads a release candidate version of the wizard into the Android marketplace through the Cisco Android marketplace publisher account.

This is the Android provisioning process:

1. Cisco uses the Software Development Kit (SDK) in order to create the Android package with a .apk extension.
2. Cisco uploads a package into the Android marketplace.
3. The user configures the policy in client provisioning with the appropriate parameters.
4. After registration of the device, the end user is redirected to the client provisioning service when dot1x authentication fails.
5. The provisioning portal page provides a button that redirects user to the Android marketplace portal where they can download the SPW.
6. The Cisco SPW is launched and performs provisioning of the supplicant:
    1. SPW discovers the ISE and downloads the profile from ISE.
    2. SPW creates a cert/key pair for EAP−TLS.
    3. SPW makes a Simple Certificate Enrollment Protocol (SCEP) proxy request call to ISE and gets the certificate.
    4. SPW applies the wireless profiles.
    5. SPW triggers re−authentication if the profiles are applied successfully.
    6. SPW exits.

Dual SSID Wireless BYOD Self−Registration

This is the process for dual SSID wireless BYOD self−registration:

1. The user associates to the Guest SSID.
2. The user opens a browser and is redirected to the ISE CWA Guest Portal.
3. The user enters an employee username and password in the Guest Portal.
4. ISE authenticates the user, and, based on the fact that they are an employee and not a guest, redirects the user to the Employee Device Registration guest page.

5. The MAC address is pre−populated in the Device Registration guest page for the DeviceID. The user enters a description and accepts the Acceptable Use Policy (AUP) if required.
6. The user selects ***Accept*** and begins to download and install the SPW.
7. The supplicant for that user's device is provisioned along with any certificates.
8. CoA occurs, and the device reassociates to the corporate SSID (CORP) and authenticates with EAP−TLS (or other authorization method in use for that supplicant).

Single SSID Wireless BYOD Self−Registration

In this scenario, there is a single SSID for corporate access (CORP) that supports both Protected Extensible Authentication Protocol (PEAP) and EAP−TLS. There is no Guest SSID.

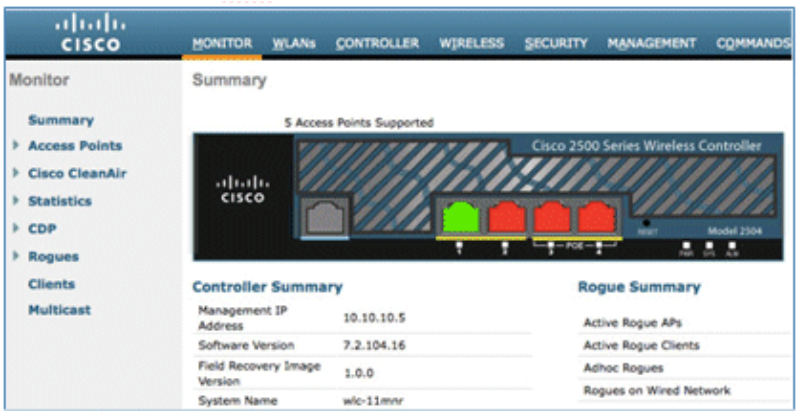
This is the process for single SSID wireless BYOD self−registration:

1. The user associates to CORP.
2. The user enters an employee username and password into the supplicant for the PEAP authentication.
3. The ISE authenticates the user, and, based on the PEAP method, provides an authorization policy of accept with redirect to the Employee Device Registration guest page.
4. The user opens a browser and is redirected to the Employee Device Registration guest page.
5. The MAC address is pre−populated in the Device Registration guest page for the DeviceID. The user enters a description and accepts the AUP.
6. The user selects ***Accept*** and begins to download and install the SPW.
7. The supplicant for that user's device is provisioned along with any certificates.
8. CoA occurs, and the device reassociates to the CORP SSID and authenticates with EAP−TLS.

Feature Configuration

Complete these steps in order to begin configuration:

1. For this guide, ensure that the WLC version is 7.2.110.0 or later.

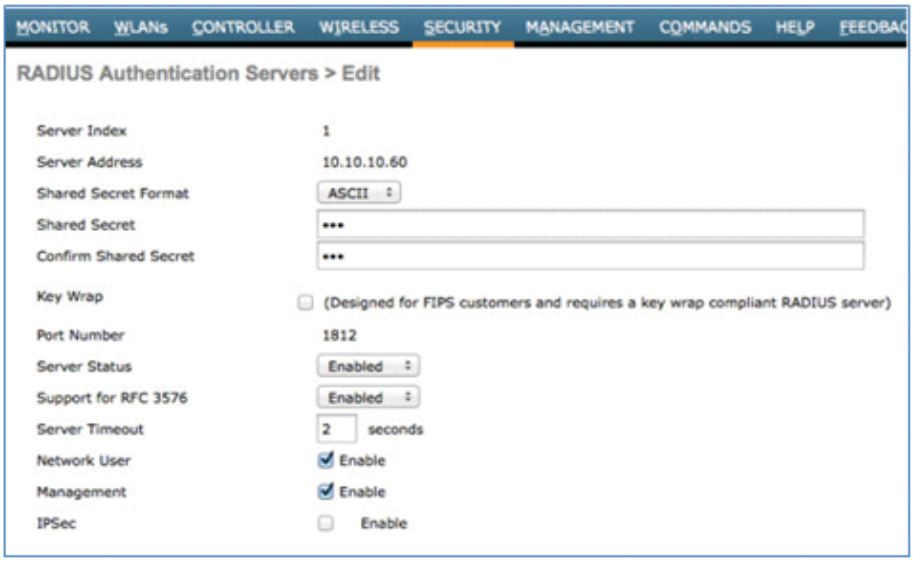


2. Navigate to ***Security*** > ***RADIUS*** > ***Authentication***, and add the RADIUS server to the WLC.

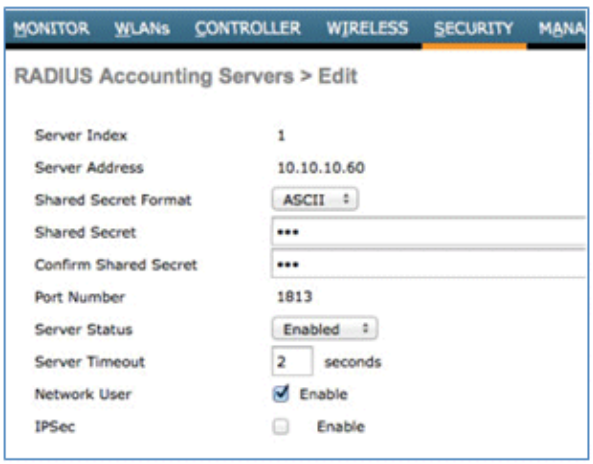


3. Add the ISE 1.1.1 to the WLC:

   - Enter a Shared Secret.
   - Set Support for RFC 3576 to ***Enabled***.



4. Add the same ISE server as a RADIUS accounting server.



5. Create a WLC Pre−Auth ACL to use in the ISE policy later. Navigate to ***WLC*** > ***Security*** > ***Access Control Lists*** > ***FlexConnect ACLs***, and create a new FlexConnect ACL named ***ACL−REDIRECT*** (in this example).



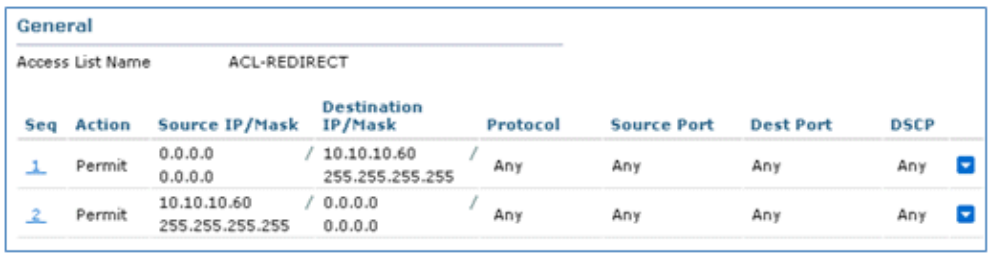
6. In the ACL rules, permit all traffic to/from the ISE, and permit client traffic during supplicant provisioning.

    a. For the first rule (sequence 1):

        ◊ Set Source to ***Any***.
        ◊ Set IP (ISE address)/ Netmask ***255.255.255.255***.
        ◊ Set Action to ***Permit***.

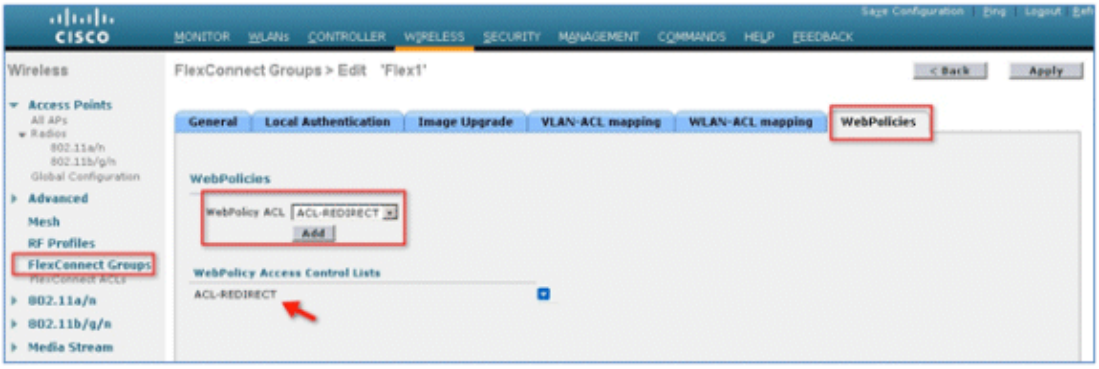


    b. For the second rule (sequence 2), set source IP (ISE address)/ mask 255.255.255.255 to ***Any*** and Action to ***Permit***.



7. Create a new FlexConnect Group named Flex1 (in this example):

    a. Navigate to ***FlexConnect Group*** > ***WebPolicies*** tab.
    b. Under the WebPolicy ACL field, click ***Add***, and select ***ACL−REDIRECT*** or the FlexConnect ACL created previously.
    c. Confirm that it populates the ***WebPolicy Access Control Lists*** field.



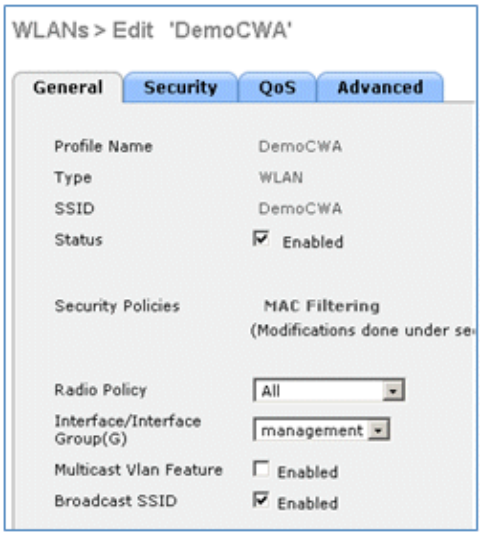
8. Click ***Apply*** and ***Save Configuration***.

WLAN Configuration

Complete these steps in order to configure the WLAN:

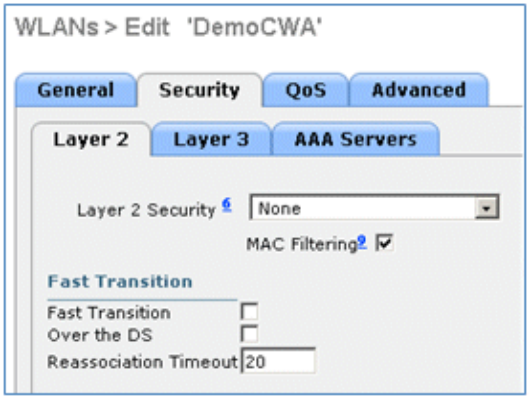
1. Create an Open WLAN SSID for the dual SSID example:

    - Enter a WLAN name: ***DemoCWA*** (in this example).
    - Select the ***Enabled*** option for Status.



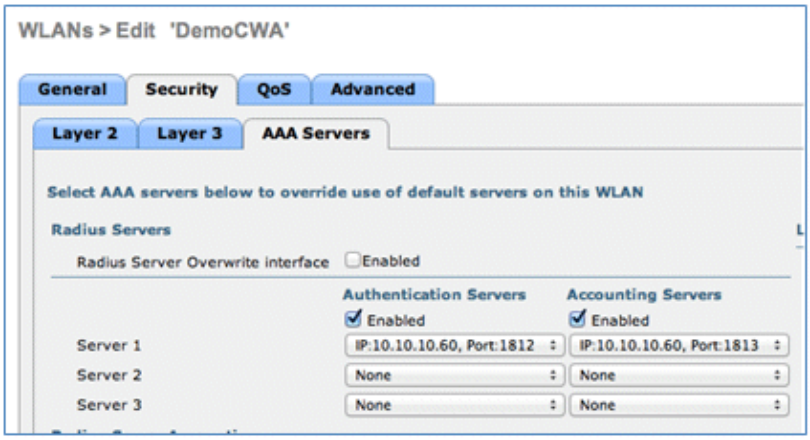
2. Navigate to the ***Security*** tab > ***Layer 2*** tab, and set these attributes:

    - Layer 2 Security: ***None***
    - MAC Filtering: ***Enabled*** (box is checked)
    - Fast Transition: ***Disabled*** (box is not checked)



3. Go to the ***AAA Servers*** tab, and set these attributes:

   - Authentication and Account Servers: ***Enabled***
   - Server 1: *<ISE IP address>*

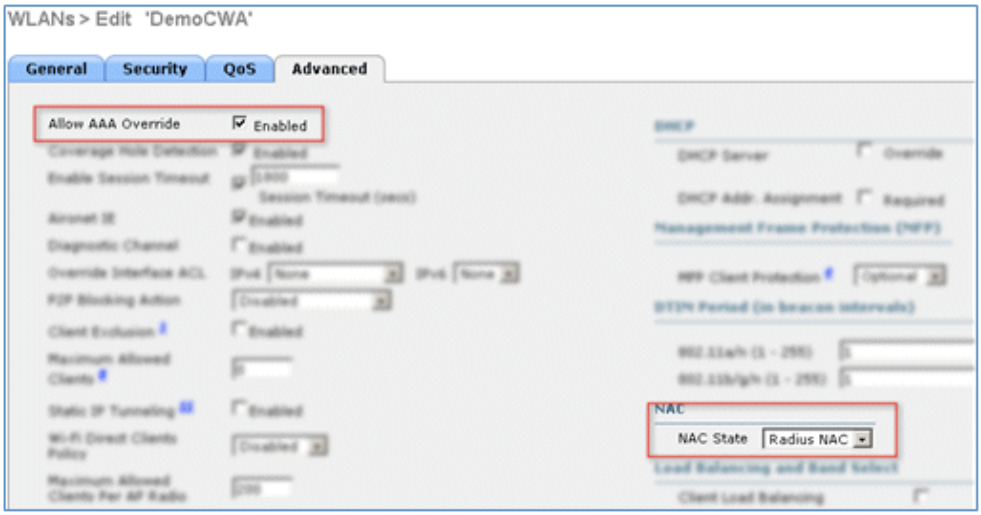


4. Scroll down from the ***AAA Servers*** tab. Under Authentication priority order for web−auth user, make sure that ***RADIUS*** is used for authentication and the others are not used.



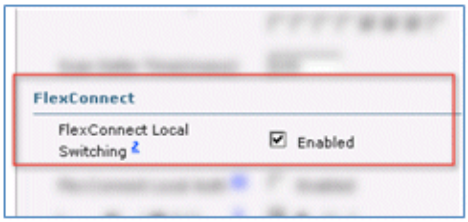
5. Go to the ***Advanced*** tab, and set these attributes:

   - Allow AAA Override: ***Enabled***
   - NAC State: ***Radius NAC***

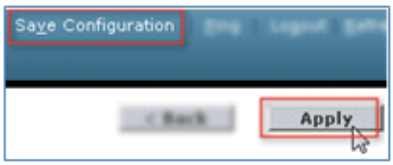


Note: RADIUS Network Admission Control (NAC) is not supported when the FlexConnect AP is in disconnected mode. Thus, if the FlexConnect AP is in standalone mode and loses connection to the WLC, all clients are disconnected, and the SSID is no longer advertised.

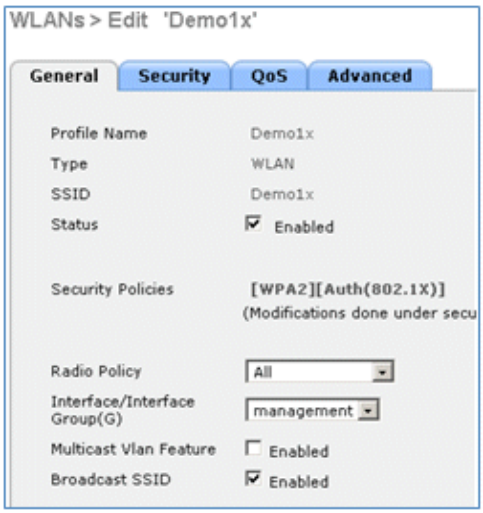
6. Scroll down in the Advanced tab, and set FlexConnect Local Switching to ***Enabled***.



7. Click ***Apply*** and ***Save Configuration***.

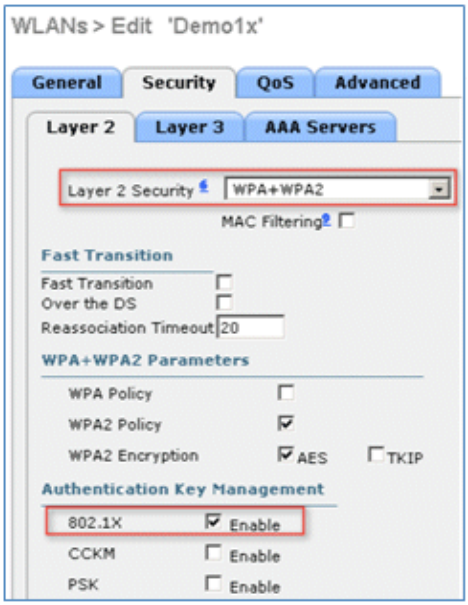


8. Create a 802.1X WLAN SSID named ***Demo1x*** (in this example) for single and dual SSID scenarios.



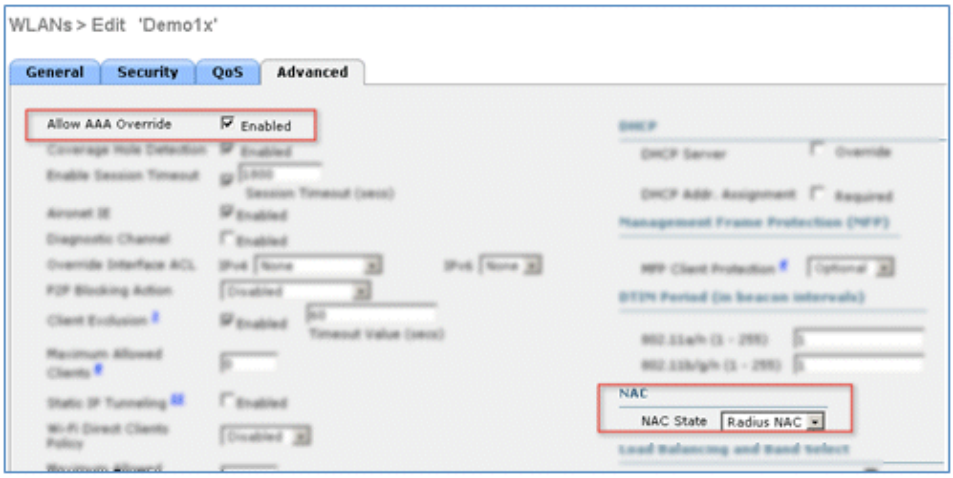
9. Navigate to the ***Security*** tab > ***Layer 2*** tab, and set these attributes:

    - Layer 2 Security: ***WPA+WPA2***
    - Fast Transition: ***Disabled*** (box is not checked)
    - Authentication Key Management: 802.lX: ***Enable***

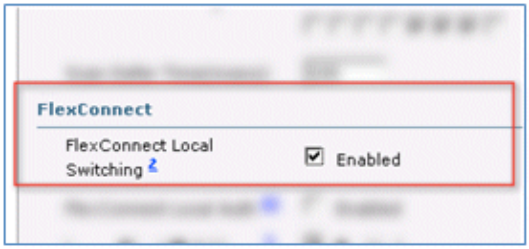


10. Go to the ***Advanced*** tab, and set these attributes:

    - Allow AAA Override: ***Enabled***
    - NAC State: ***Radius NAC***



11. Scroll down in the ***Advanced*** tab, and set FlexConnect Local Switching to ***Enabled***.



12. Click ***Apply*** and ***Save Configuration***.



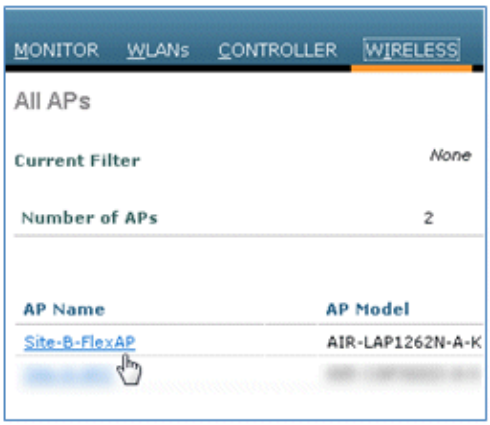
13. Confirm that both of the new WLANs were created.



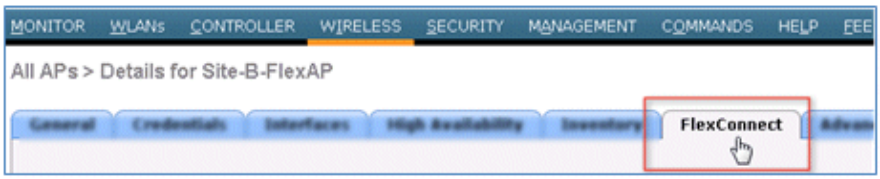
FlexConnect AP Configuration

Complete these steps in order to configure the FlexConnect AP:

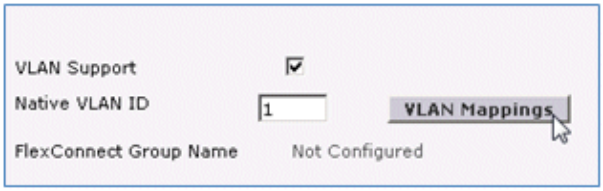
1. Navigate to ***WLC*** > ***Wireless***, and click the target FlexConnect AP.



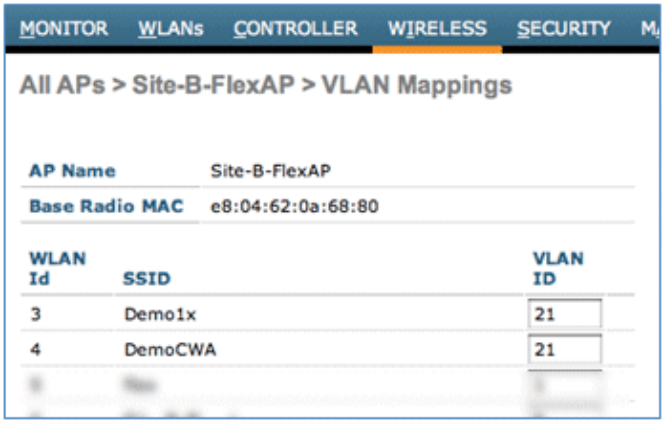
2. Click the ***FlexConnect*** tab.



3. Enable VLAN Support (box is checked), set the Native VLAN ID, and click ***VLAN Mappings***.



4. Set the VLAN ID to ***21*** (in this example) for the SSID for local switching.



5. Click ***Apply*** and ***Save Configuration***.

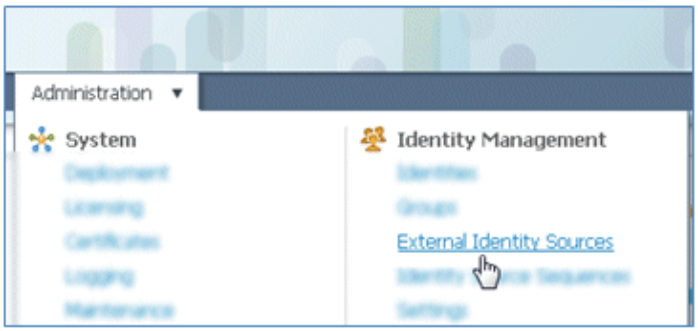
ISE Configuration

Complete these steps in order to configure the ISE:

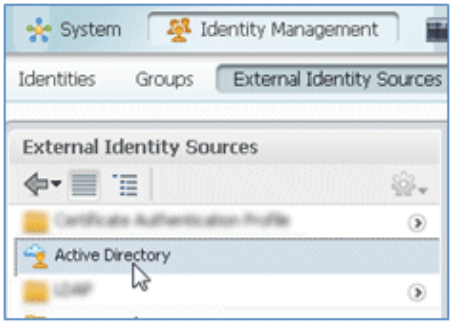
1. Log in to the ISE server: <*https://ise*>.



2. Navigate to ***Administration*** > ***Identity Management*** > ***External Identity Sources***.

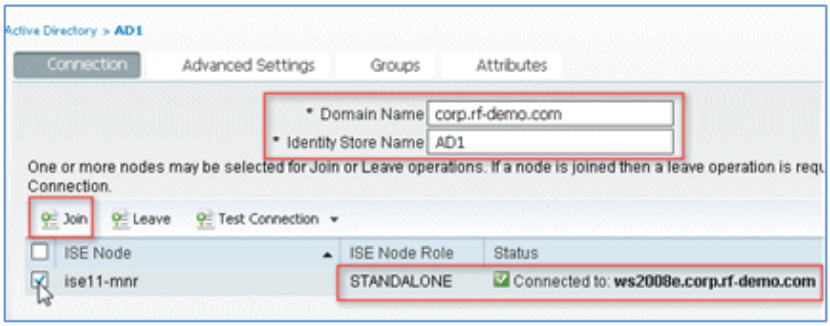


3. Click ***Active Directory***.

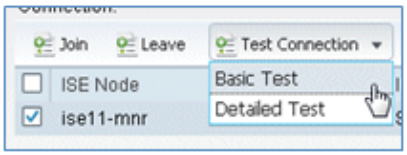


4. In the Connection tab:

   a. Add the Domain Name of ***corp.rf−demo.com*** (in this example), and change the Identity Store Name default to ***AD1***.
   b. Click ***Save Configuration***.
   c. Click ***Join***, and provide the AD Administrator account username and password required to join.
   d. The Status must be green. Enable ***Connected to:*** (box is checked).

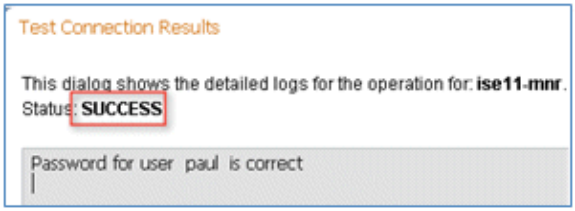


5. Perform a basic connection test to the AD with a current domain user.



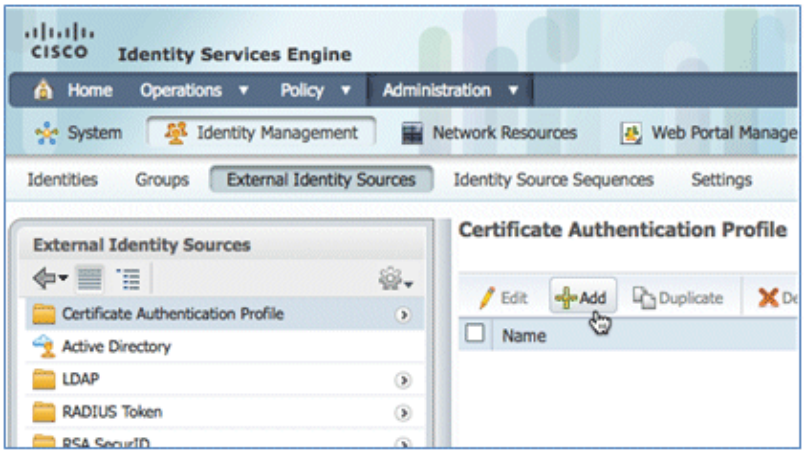


6. If the connection to the AD is successful, a dialog confirms that the password is correct.

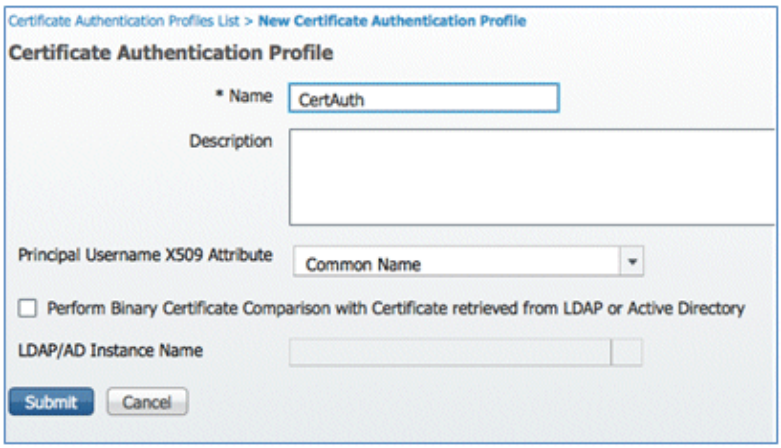


7. Navigate to ***Administration*** > ***Identity Management*** > ***External Identity Sources***:

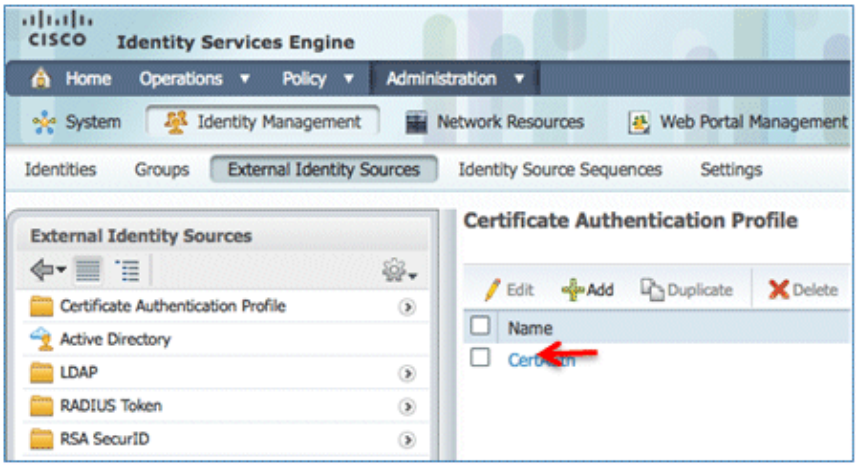
    a. Click ***Certificate Authentication Profile***.
    b. Click ***Add*** for a new Certificate Authentication Profile (CAP).



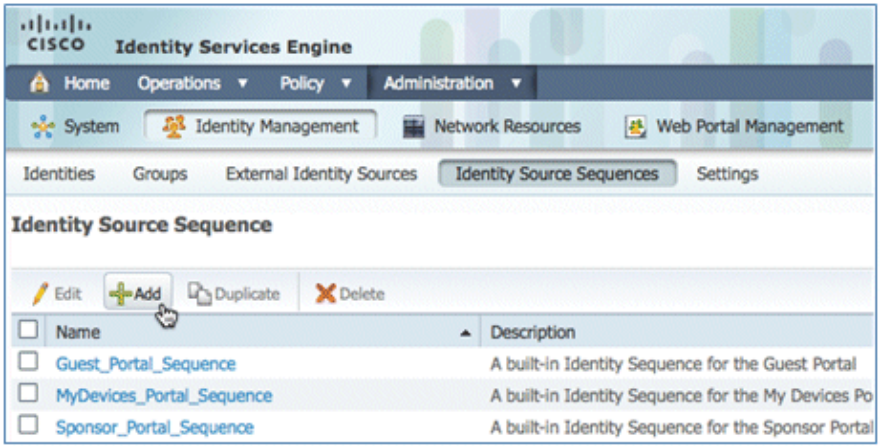
8. Enter a name of ***CertAuth*** (in this example) for the CAP; for the Principal Username X509 Attribute, select ***Common Name***; then, click ***Submit***.



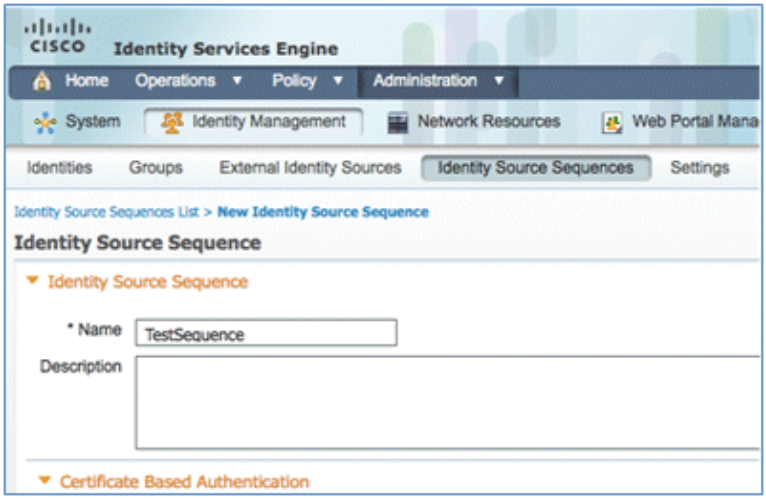
9. Confirm that the new CAP is added.



10. Navigate to ***Administration*** > ***Identity Management*** > ***Identity Source Sequences***, and click ***Add*** .

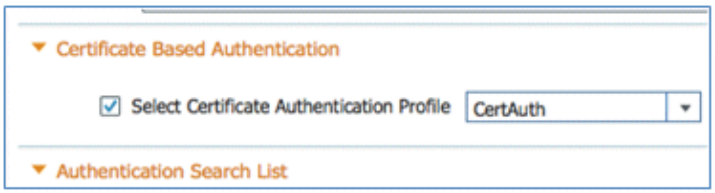


11. Give the sequence a name of ***TestSequence*** (in this example).



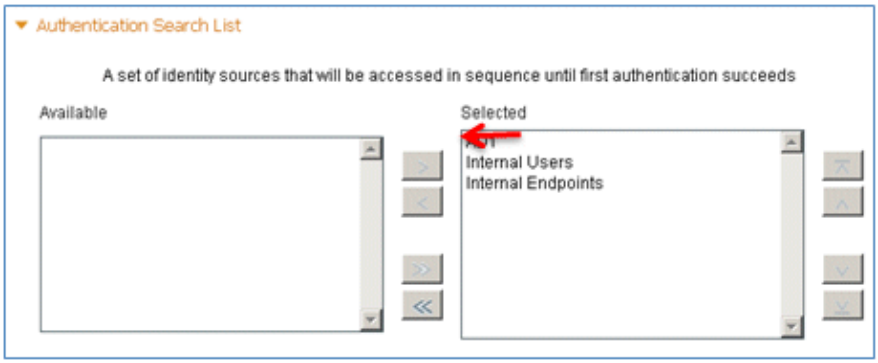
12. Scroll down to ***Certificate Based Authentication***:

    a. Enable ***Select Certificate Authentication Profile*** (box is checked).
    b. Select ***CertAuth*** (or another CAP profile created earlier).

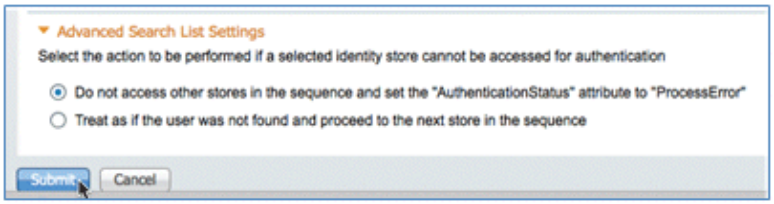


13. Scroll down to ***Authentication Search List***:

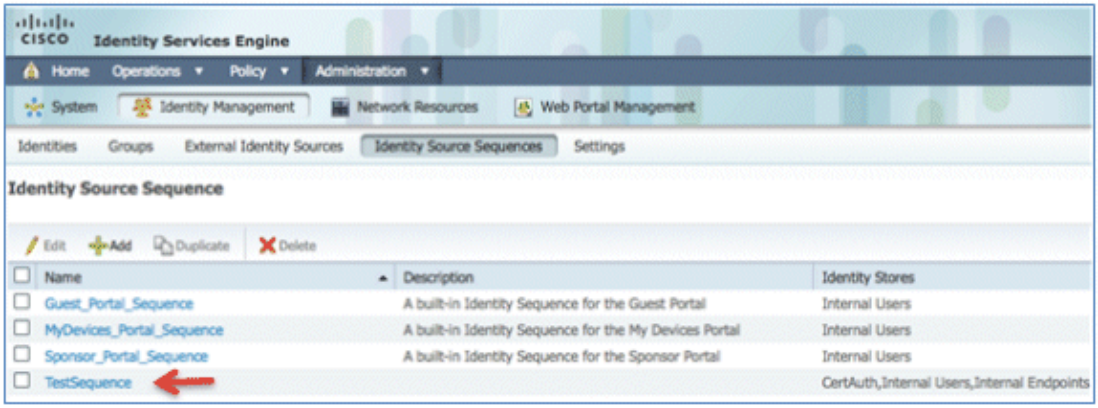
    a. Move AD1 from Available to Selected.
    b. Click the up button in order to move AD1 to the top priority.



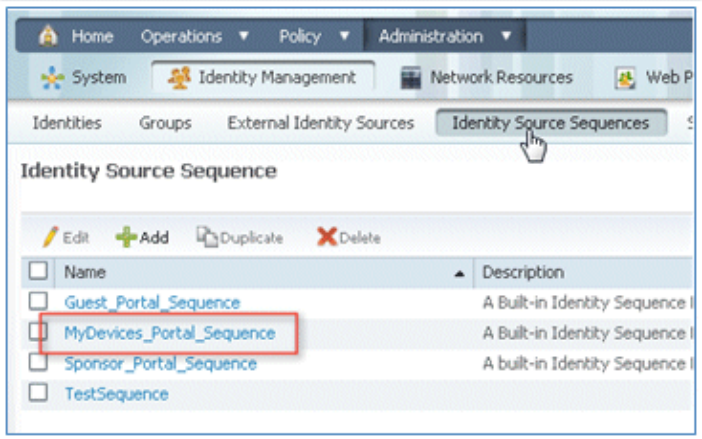
14. Click ***Submit*** in order to save.



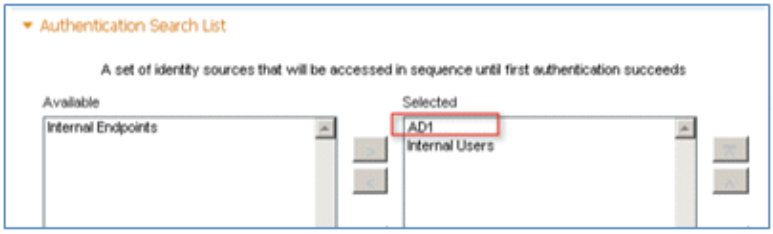
15. Confirm that the new Identity Source Sequence is added.



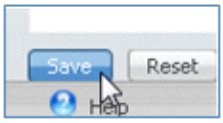
16. Use the AD in order to authenticate the My Devices Portal. Navigate to ***ISE*** > ***Administration*** > ***Identity Management*** > ***Identity Source Sequence***, and edit ***MyDevices_Portal_Sequence***.



17. Add ***AD1*** to the Selected list, and click the up button in order to move AD1 to the top priority.



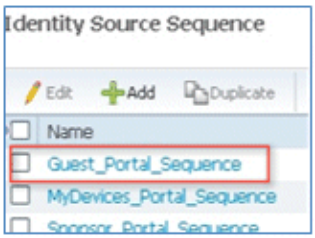
18. Click ***Save***.



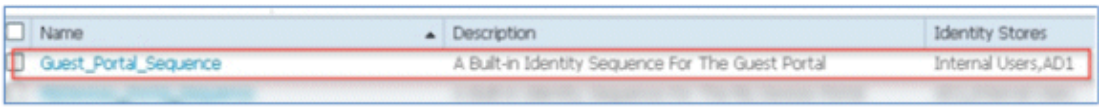
19. Confirm that the Identity Store sequence for MyDevices_Portal_Sequence contains ***AD1***.



20. Repeat steps 16−19 in order to add AD1 for Guest_Portal_Sequence, and click ***Save***.



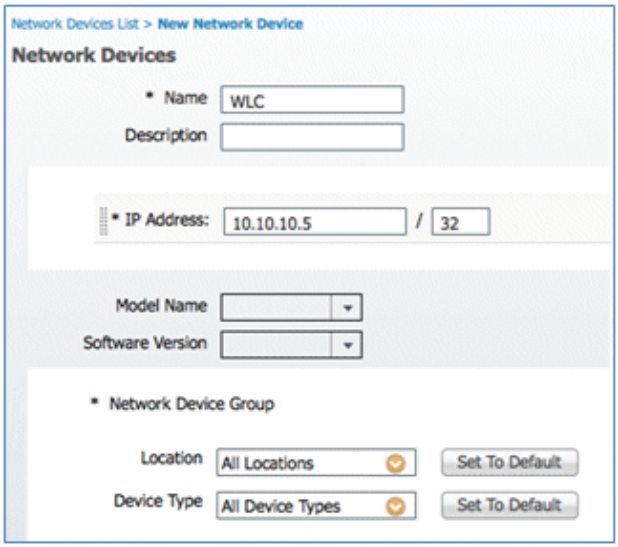
21. Confirm that Guest_Portal_Sequence contains ***AD1***.



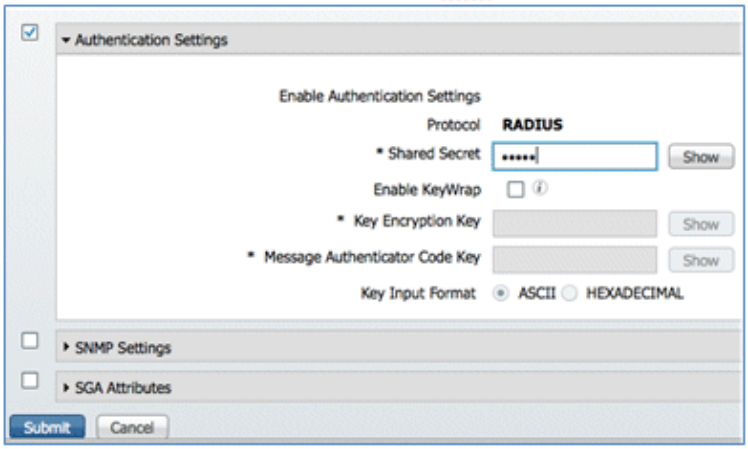
22. In order to add the WLC to Network Access Device (WLC), navigate to ***Administration*** > ***Network Resources*** > ***Network Devices***, and click ***Add***.



23. Add the WLC name, IP address, Subnet Mask, and so forth.

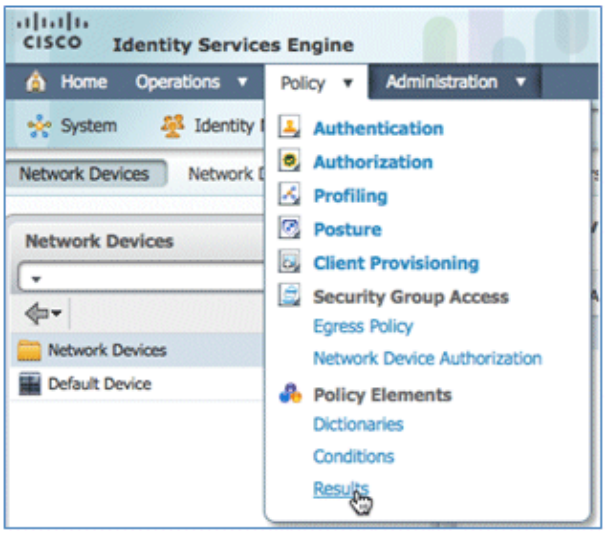


24. Scroll down to Authentication Settings, and enter the Shared Secret. This must match the shared secret of the WLC RADIUS.

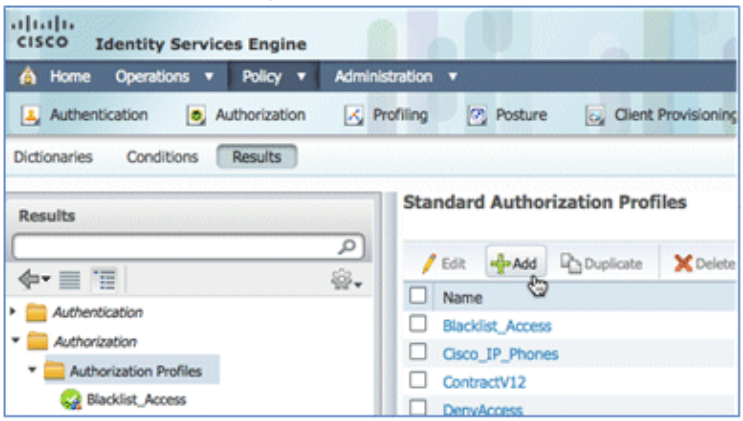


25. Click ***Submit***.

26. Navigate to ***ISE*** > ***Policy*** > ***Policy Elements*** > ***Results***.

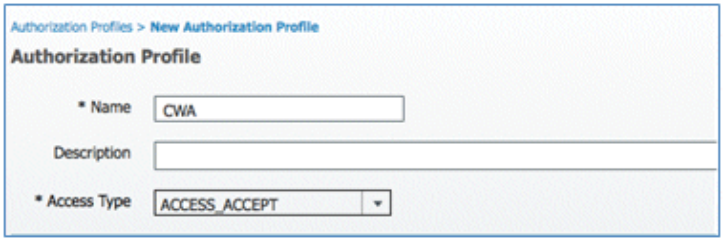


27. Expand ***Results*** and ***Authorization***, click ***Authorization Profiles***, and click ***Add*** for a new profile.



28. Give this profile these values:

- Name: ***CWA***

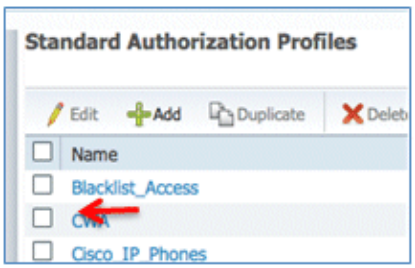


- Enable Web Authentication (box is checked):

  - Web Authentication: ***Centralized***
  - ACL: ***ACL−REDIRECT*** (This must match the WLC pre−auth ACL name.)
  - Redirect: ***Default***



29. Click ***Submit***, and confirm that the CWA authorization profile has been added.

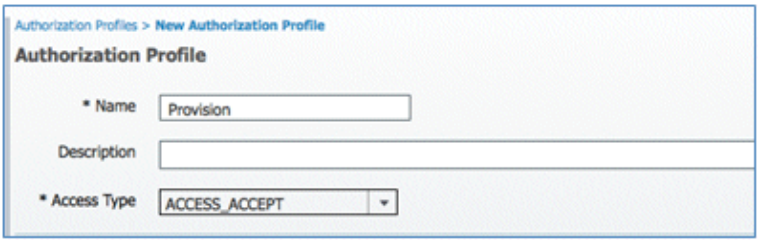


30. Click ***Add*** in order to create a new authorization profile.



31. Give this profile these values:

- Name: ***Provision***

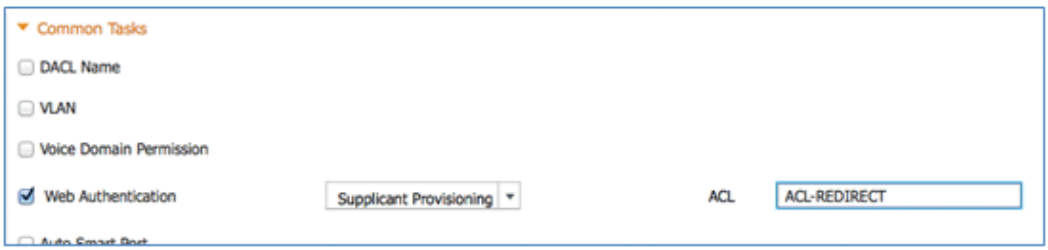


- Enable Web Authentication (box is checked):

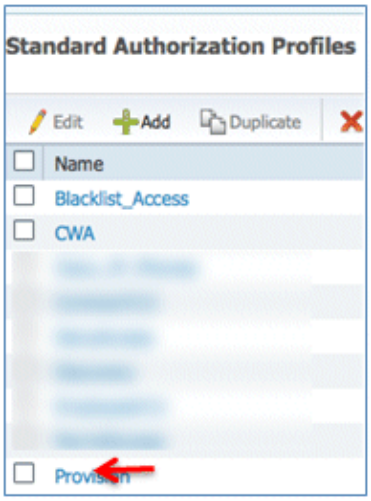
  - Web Authentication Value: ***Supplicant Provisioning***



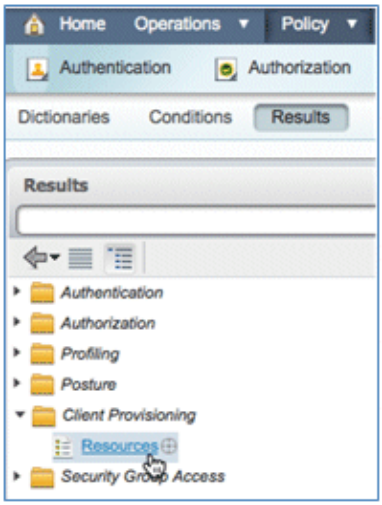
  - ACL: ***ACL−REDIRECT*** (This must match the WLC pre−auth ACL name.)



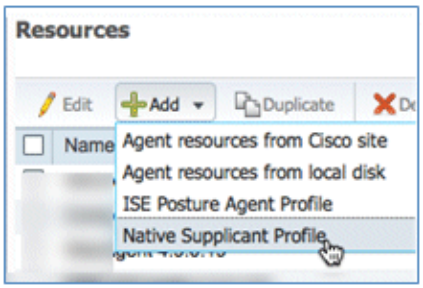
32. Click ***Submit***, and confirm that the Provision authorization profile was added.



33. Scroll down in Results, expand ***Client Provisioning***, and click ***Resources***.



34. Select ***Native Supplicant Profile***.

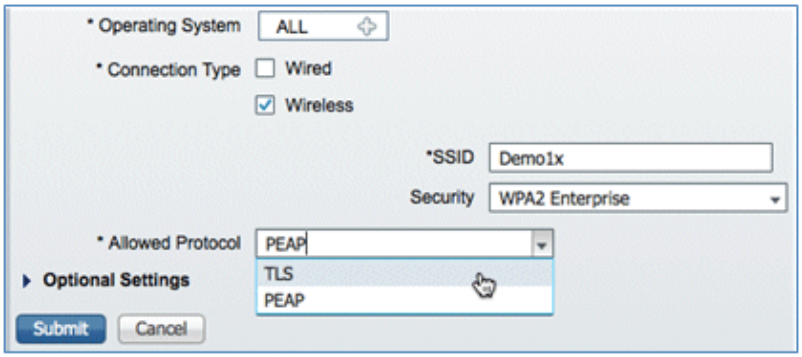


35. Give the Profile a name of ***WirelessSP*** (in this example).



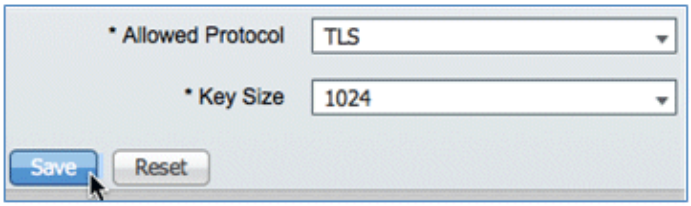
36. Enter these values:

- Connection Type: ***Wireless***
- SSID: ***Demo1x*** (this value is from the WLC 802.1x WLAN configuration)
- Allowed Protocol: ***TLS***
- Key Size: ***1024***

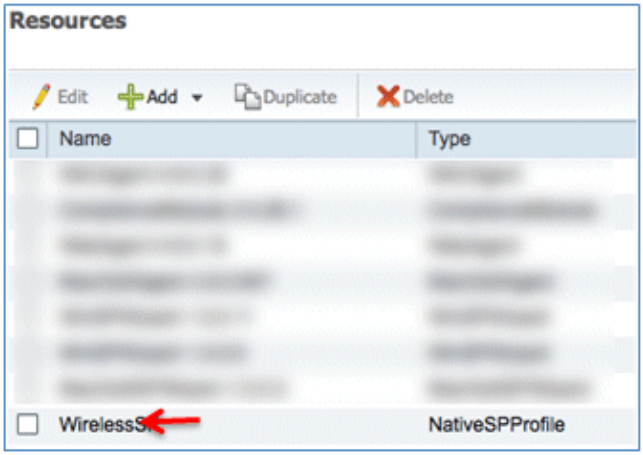


37. Click ***Submit***.

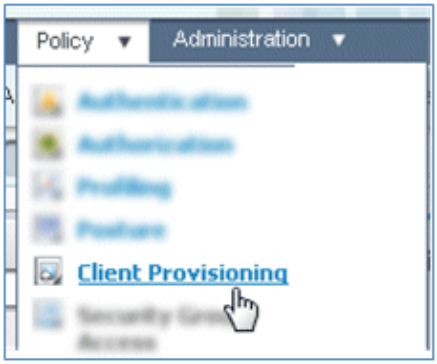
38. Click ***Save***.



39. Confirm that the new profile has been added.

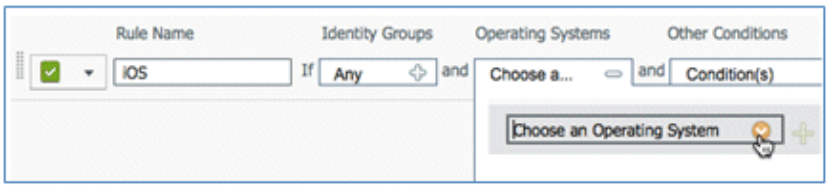


40. Navigate to ***Policy*** > ***Client Provisioning***.

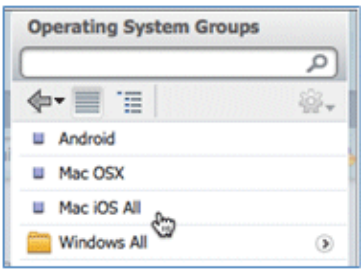


41. Enter these values for the provisioning rule of iOS devices:

- ♦ Rule Name: ***iOS***
- ♦ Identity Groups: ***Any***



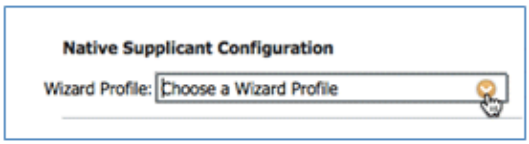
- ♦ Operating Systems: ***Mac iOS All***

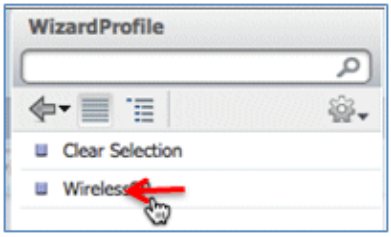


- ♦ Results: ***WirelessSP*** (this is the Native Supplicant Profile created earlier)

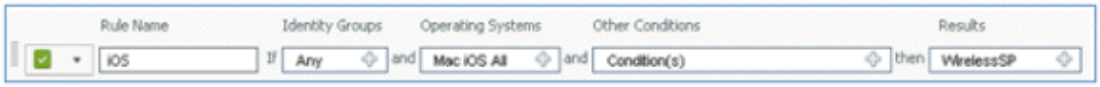


◊ Navigate to ***Results*** > ***Wizard Profile*** (drop−down list) > ***WirelessSP***.

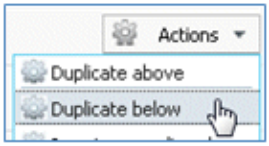




42. Confirm that the iOS Provisioning Profile was added.



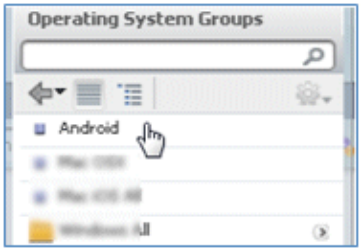
43. On the right side of the first rule, locate the Actions drop−down list, and select ***Duplicate below*** (or above).



44. Change the Name of the new rule to ***Android***.

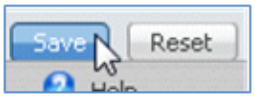


45. Change the Operating Systems to ***Android***.

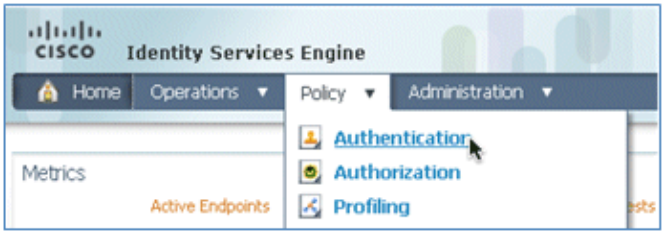


46. Leave other values unchanged.

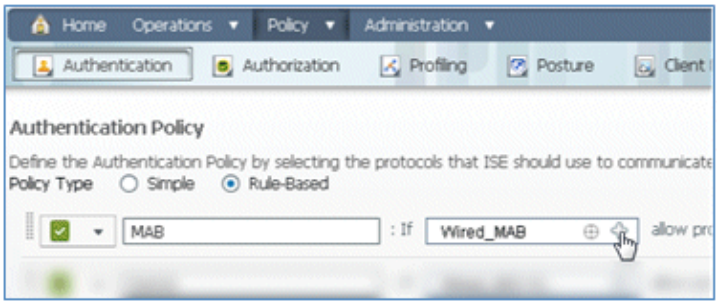
47. Click ***Save*** (lower left screen).



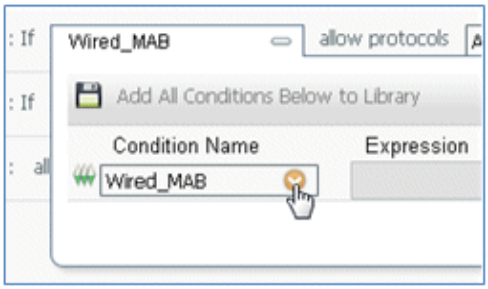
48. Navigate to ***ISE*** > ***Policy*** > ***Authentication***.



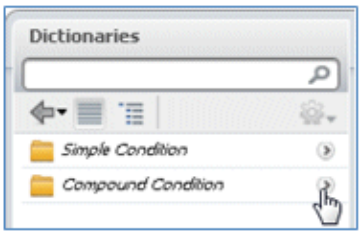
49. Modify the condition to include Wireless_MAB, and expand ***Wired_MAB***.



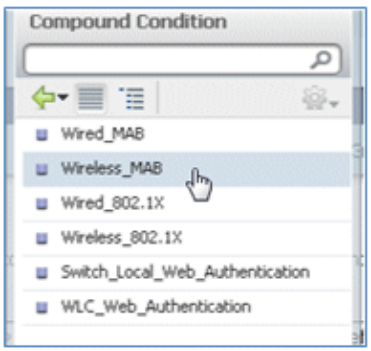
50. Click the ***Condition Name*** drop−down list.



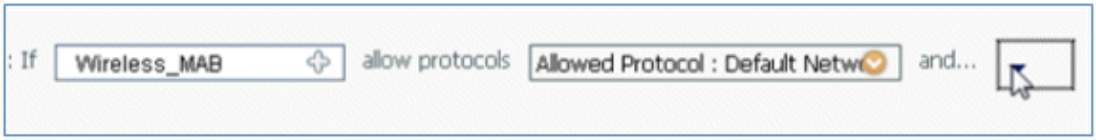
51. Select ***Dictionaries*** > ***Compound Condition***.



52. Select ***Wireless_MAB***.

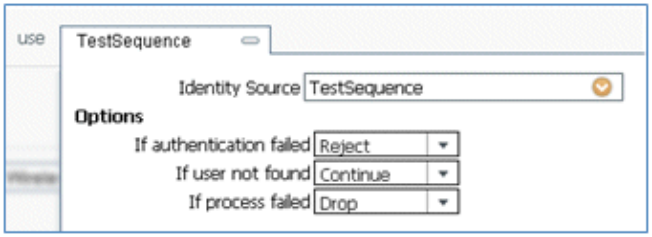


53. To the right of the rule, select the arrow to expand.

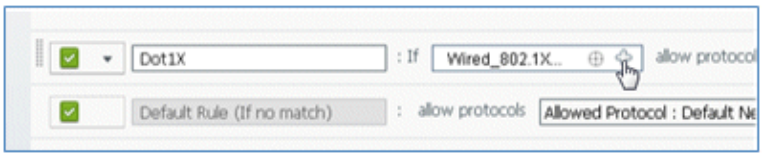


54. Select these values from the drop−down list:

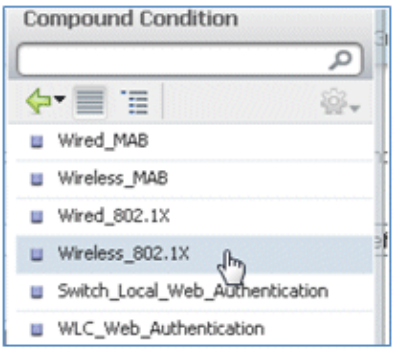
- Identity Source: ***TestSequence*** (this is the value created earlier)
- If authentication failed: ***Reject***
- If user not found: ***Continue***
- If process failed: ***Drop***

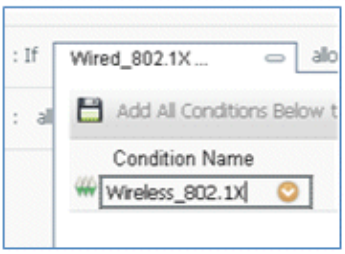


55. Go to the ***Dot1X*** rule, and change these values:

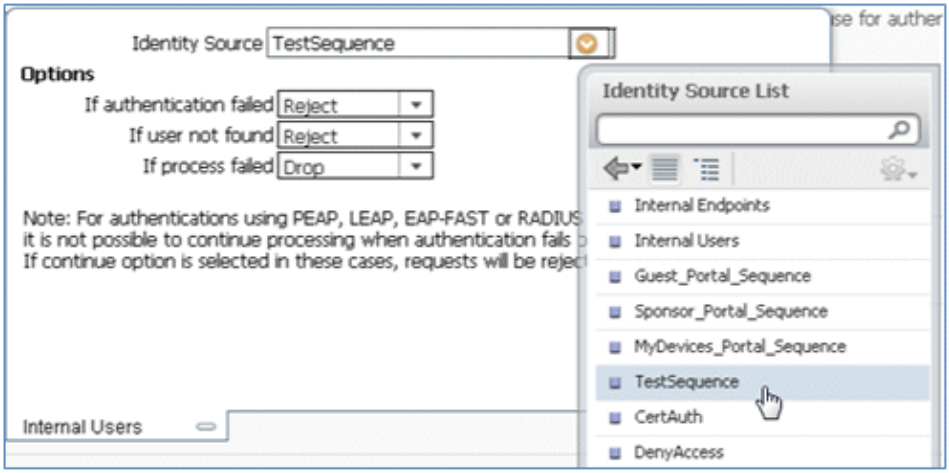


- Condition: ***Wireless_802.1X***





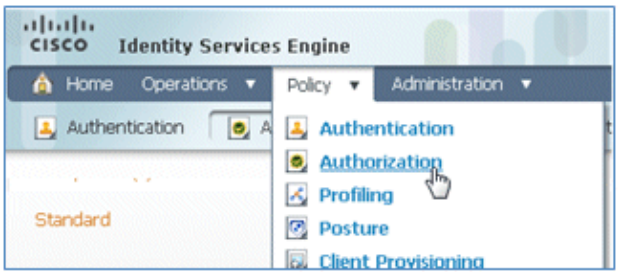
- Identity Source: ***TestSequence***



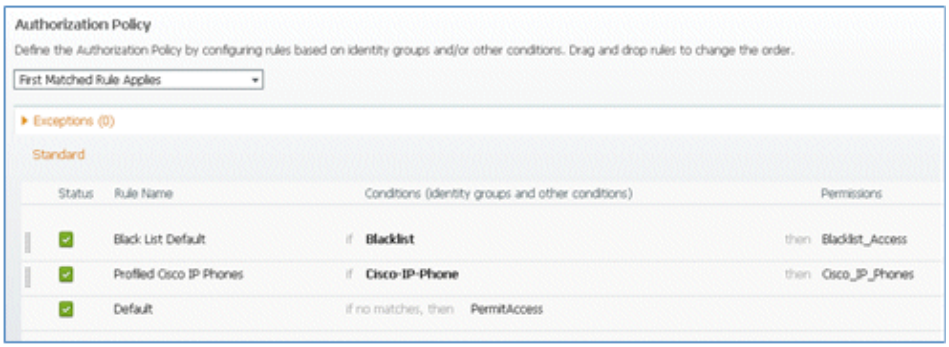
56. Click ***Save***.



57. Navigate to ***ISE*** > ***Policy*** > ***Authorization***.



58. Default rules (such as Black List Default, Profiled, and Default) are already configured from installation; the first two can be ignored; the Default rule will be edited later.



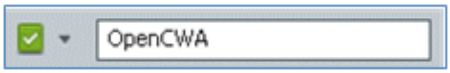
59. To the right of the second rule (Profiled Cisco IP Phones), click the down arrow next to Edit, and select ***Insert New Rule Below***.



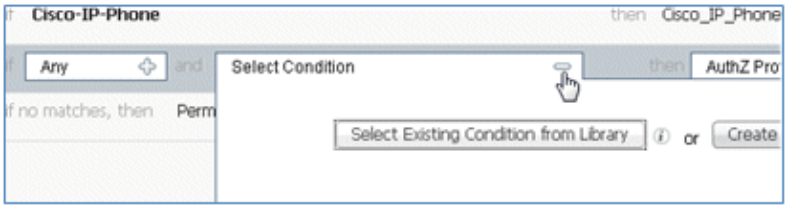
A new Standard Rule # is added.



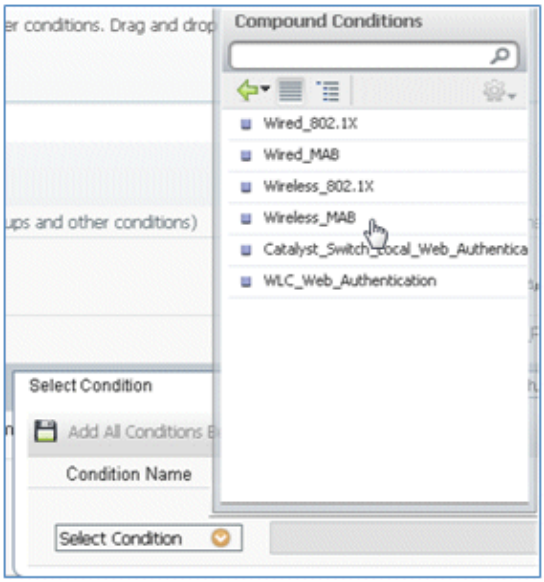
60. Change the Rule Name from Standard Rule # to ***OpenCWA***. This rule initiates the registration process on the open WLAN (dual SSID) for users that come to the guest network in order to have devices provisioned.



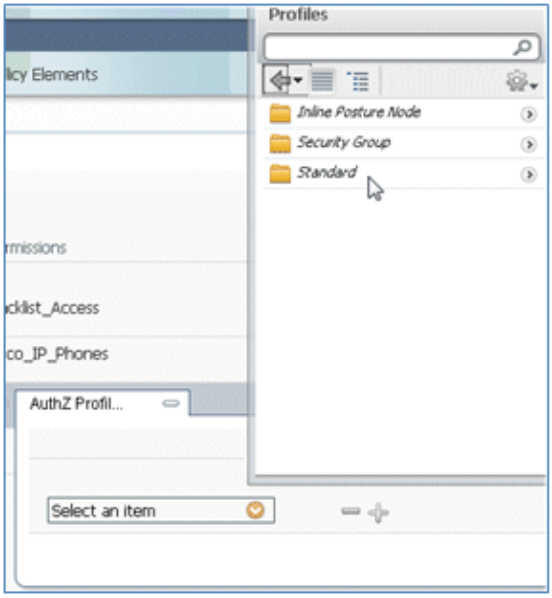
61. Click the plus sign (+) for Condition(s), and click ***Select Existing Condition from Library***.



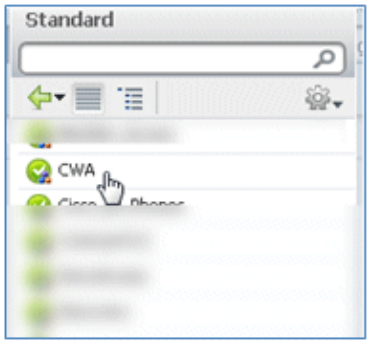
62. Select ***Compound Conditions*** > ***Wireless_MAB***.



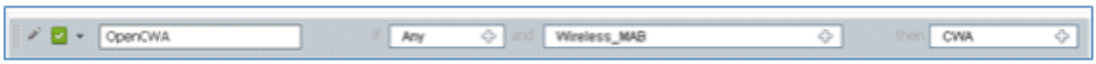
63. In the AuthZ Profile, click the plus sign (+), and select ***Standard***.



64. Select the standard ***CWA*** (this is the Authorization Profile created earlier).



65. Confirm that the rule is added with the correct Conditions and Authorization.



66. Click ***Done*** (on the right side of the rule).



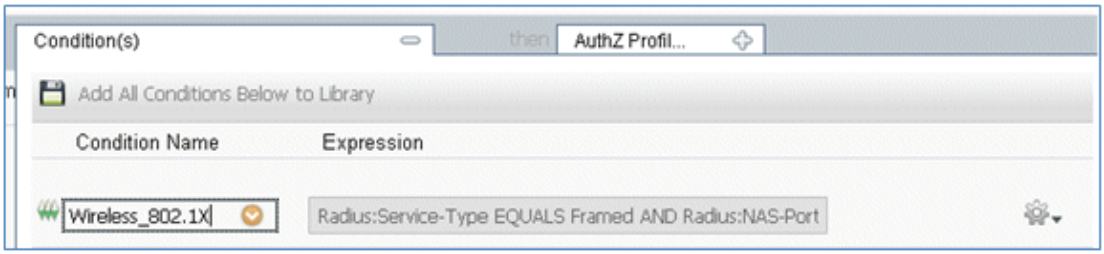
67. To the right of the same rule, click the down arrow next to Edit, and select ***Insert New Rule Below***.



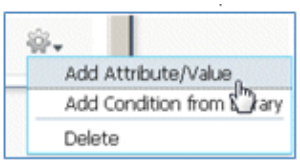
68. Change the Rule Name from Standard Rule # to ***PEAPrule*** (in this example). This rule is for PEAP (also used for single SSID scenario) to check that authentication of 802.1X without Transport Layer Security (TLS) and that network supplicant provisioning is initiated with the Provision authorization profile created previously.



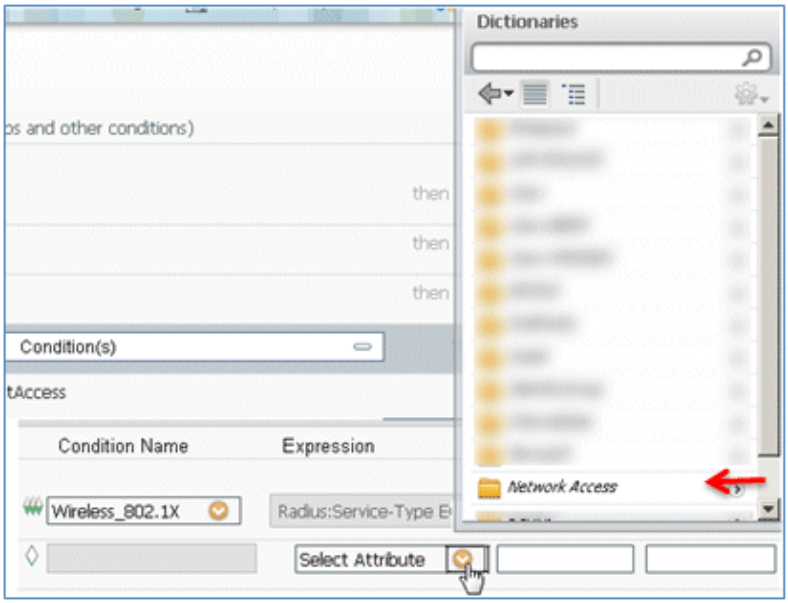
69. Change the Condition to ***Wireless_802.1X***.



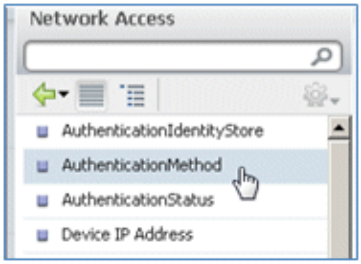
70. Click the gear icon on the right side of the condition, and select ***Add Attribute/Value***. This is an 'and' condition, not an 'or' condition.



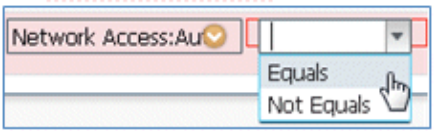
71. Locate and select ***Network Access***.



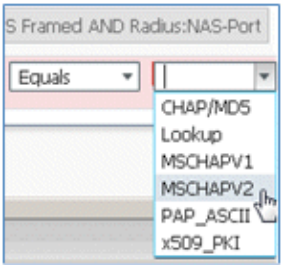
72. Select ***AuthenticationMethod***, and enter these values:



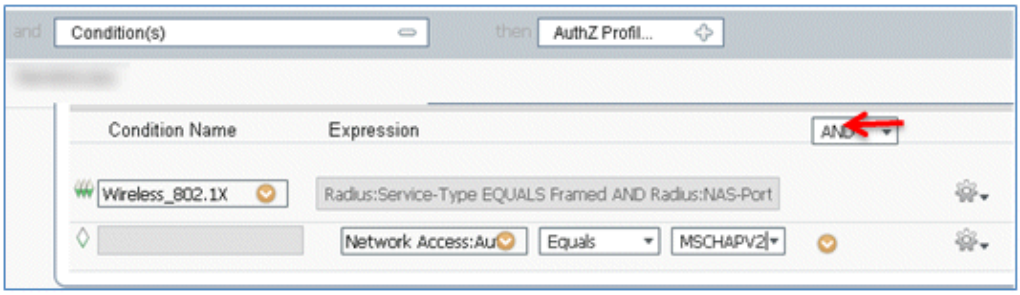
- AuthenticationMethod: ***Equals***



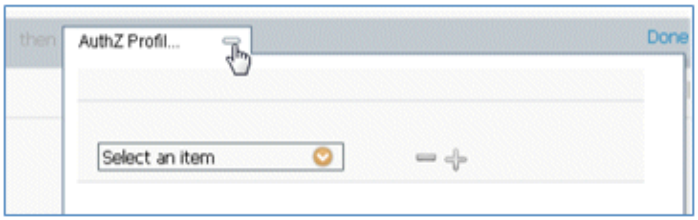
- Select ***MSCHAPV2***.

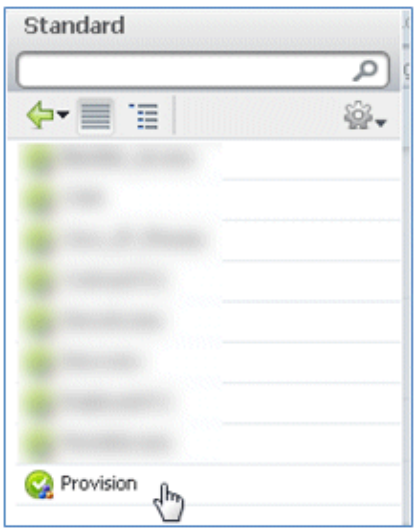


This is an example of the rule; be sure to confirm that the Condition is an AND.



73. In AuthZ Profile, select ***Standard*** > ***Provision*** (this is the Authorization Profile created earlier).





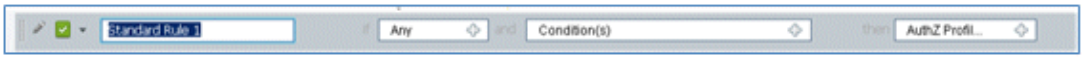
74. Click ***Done***.



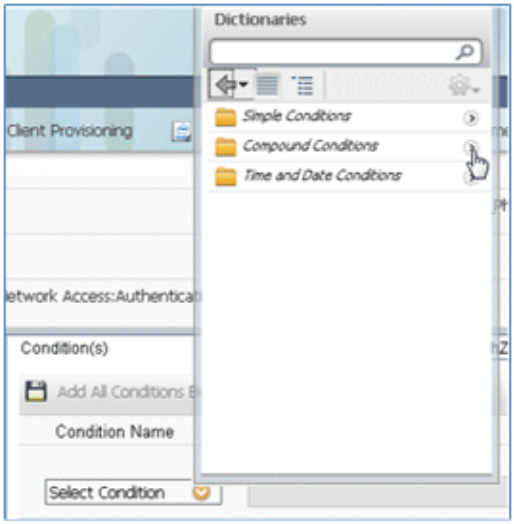
75. To the right of the PEAPrule, click the down arrow next to Edit, and select ***Insert New Rule Below***.



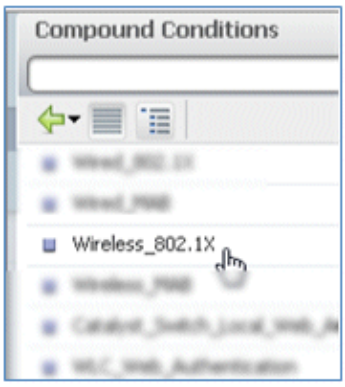
76. Change the Rule Name from Standard Rule # to ***AllowRule*** (in this example). This rule will be used in order to permit access to registered devices with certificates installed.



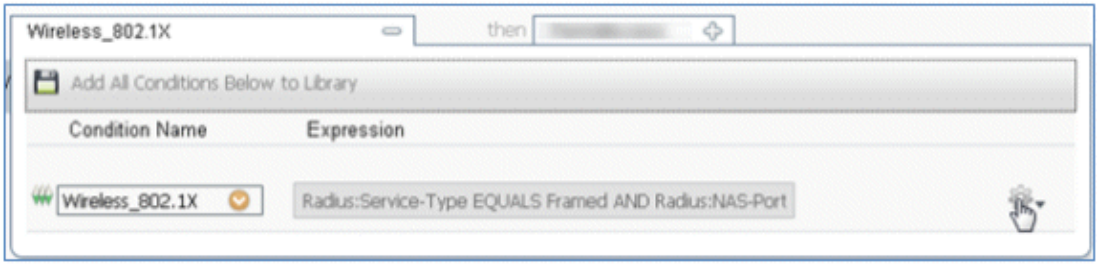
77. Under Condition(s), select ***Compound Conditions***.



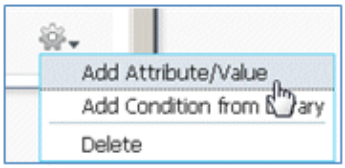
78. Select ***Wireless_802.1X***.



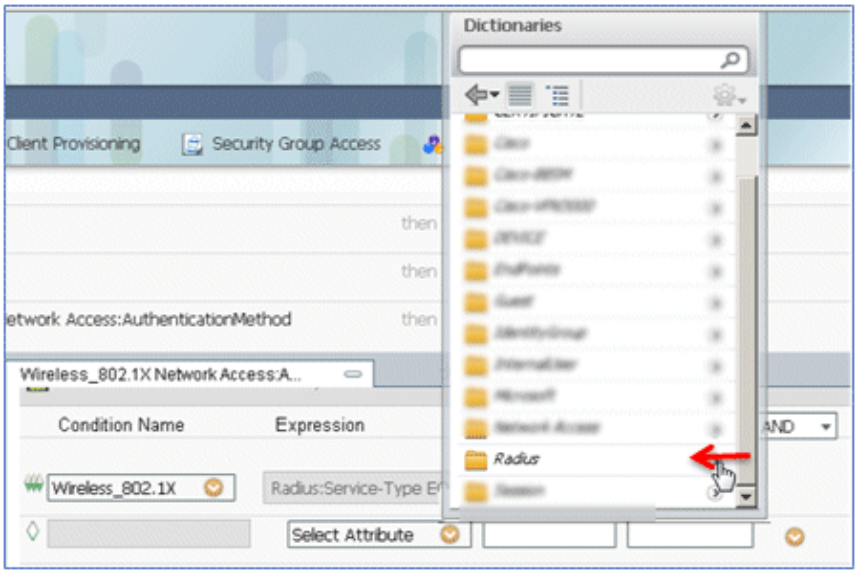
79. Add an AND attribute.



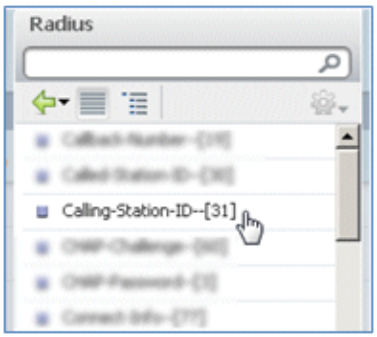
80. Click the gear icon on the right side of the condition, and select ***Add Attribute/Value***.



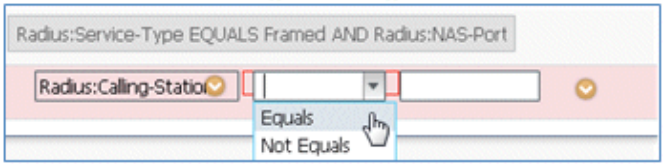
81. Locate and select ***Radius***.



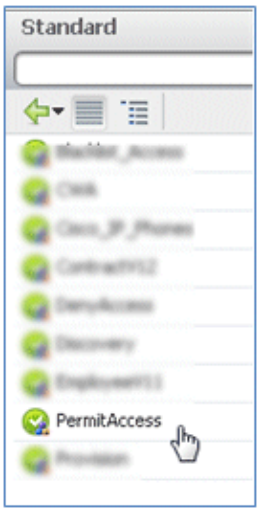
82. Select ***Calling−Station−ID−−[31]***.



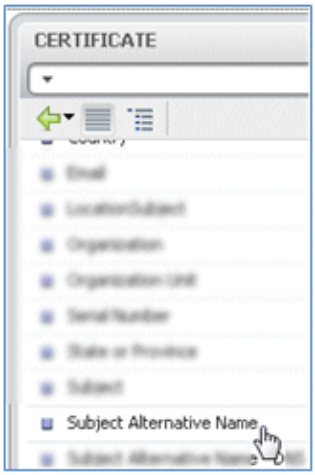
83. Select ***Equals***.



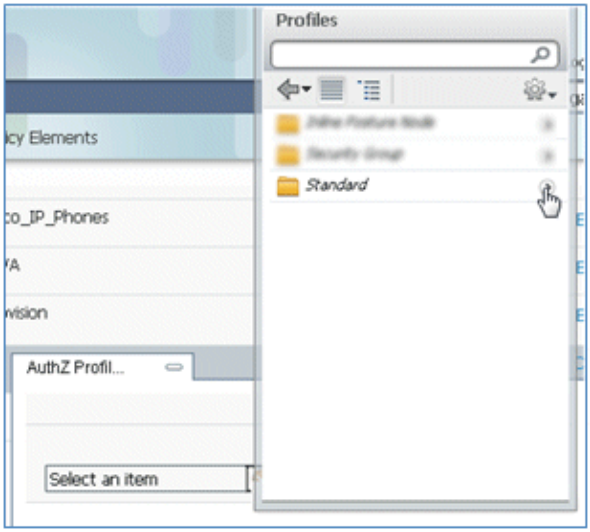
84. Go to ***CERTIFICATE***, and click the right arrow.



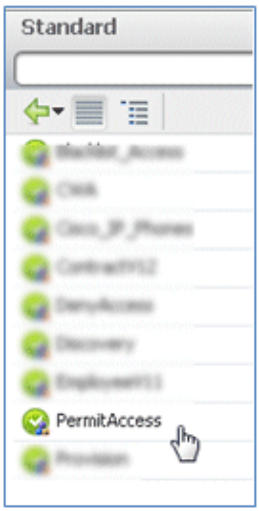
85. Select ***Subject Alternative Name***.



86. For the AuthZ Profile, select ***Standard***.



87. Select ***Permit Access***.



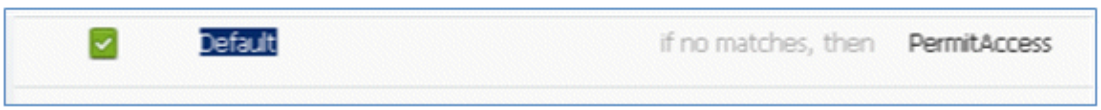
88. Click ***Done***.



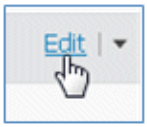
This is an example of the rule:



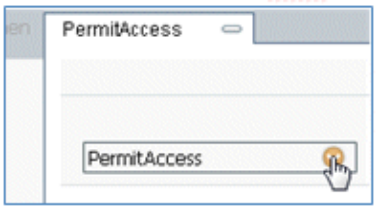
89. Locate the Default rule in order to change PermitAccess to DenyAccess.



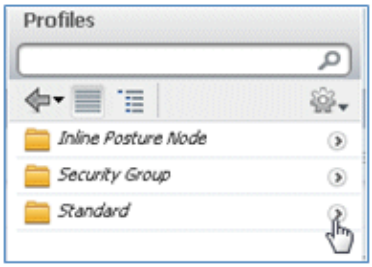
90. Click ***Edit*** in order to edit the Default rule.



91. Go to the existing AuthZ profile of PermitAccess.



92. Select ***Standard***.



93. Select ***DenyAccess***.



94. Confirm that the Default rule has DenyAccess if no matches are found.



95. Click ***Done***.



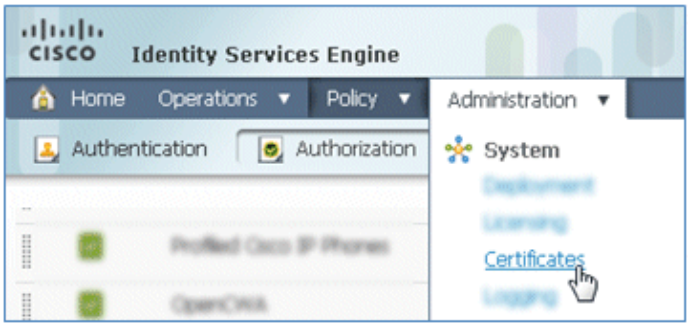
This is an example of the main rules required for this test; they are applicable for either a single SSID or dual SSID scenario.



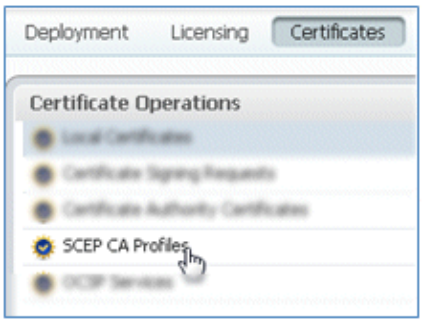
96. Click ***Save***.



97. Navigate to ***ISE*** > ***Administration*** > ***System*** > ***Certificates*** in order to configure the ISE server with a SCEP profile.



98. In Certificate Operations, click ***SCEP CA Profiles***.



99. Click ***Add***.



100. Enter these values for this profile:

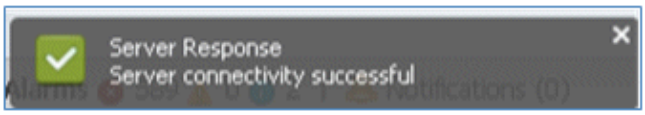
- Name: ***mySCEP*** (in this example)
- URL: ***https://***<*ca−server*>***/CertSrv/mscep/*** (Check your CA server configuration for the correct address.)



101. Click ***Test Connectivity*** in order to test connectivity of the SCEP connection.



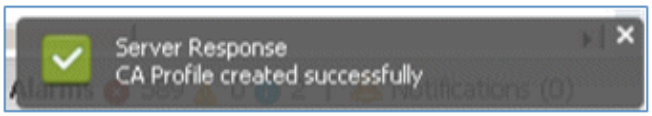
102. This response shows that the server connectivity is successful.



103. Click ***Submit***.



104. The server responds that the CA Profile was created successfully.



105. Confirm that the SCEP CA Profile is added.



User Experience − Provisioning iOS

Dual SSID

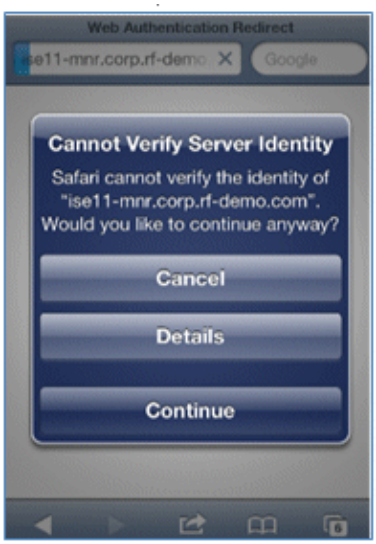
This section covers dual SSID and describes how to connect to the guest to be provisioned and how to connect to a 802.1x WLAN.

Complete these steps in order to provision iOS in the dual SSID scenario:

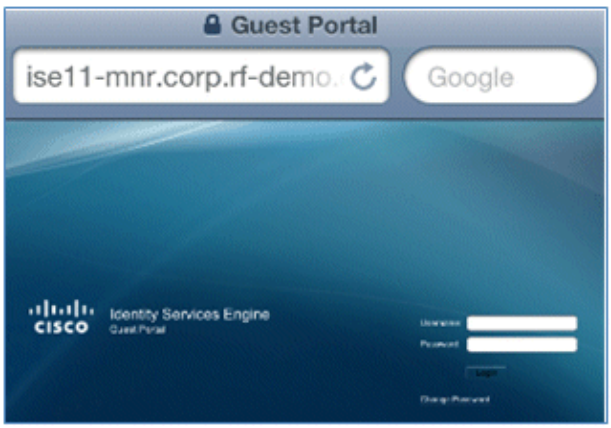
1. On the iOS device, go to ***Wi−Fi Networks***, and select ***DemoCWA*** (configured open WLAN on WLC).



2. Open the Safari browser on the iOS device, and visit a reachable URL (for example, internal/external webserver). The ISE redirects you to the portal. Click ***Continue***.



3. You are redirected to the Guest Portal for login.



4. Log in with an AD user account and password. Install the CA Profile when prompted.



5. Click ***Install*** trusted certificate of the CA server.



6. Click ***Done*** once the profile is completely installed.



7. Return to the browser, and click ***Register***. Make a note of the Device ID that contains the MAC address of the device.



8. Click ***Install*** in order to install the verified profile.



9. Click ***Install Now***.



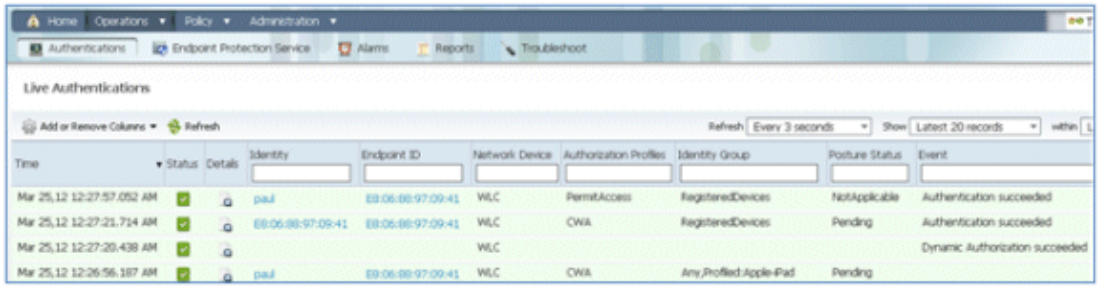
10. After the process is completed, the WirelessSP profile confirms that the profile is installed. Click ***Done***.



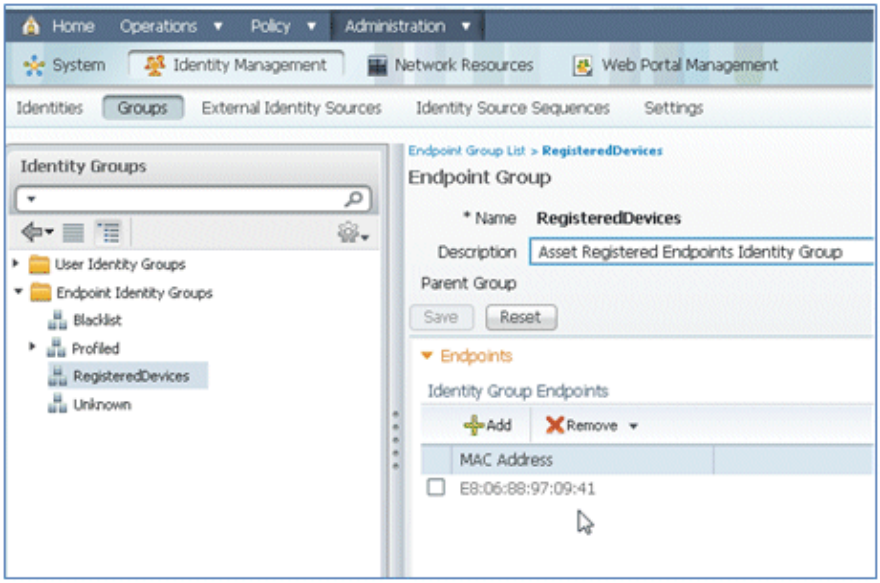
11. Go to ***Wi−Fi Networks***, and change the network to ***Demo1x***. Your device is now connected and uses TLS.



12. On the ISE, navigate to ***Operations*** > ***Authentications***. The events show the process in which the device is connected to the open guest network, goes through the registration process with supplicant provisioning, and is allowed permit access after registration.



13. Navigate to ***ISE*** > ***Administration*** > ***Identity Management*** > ***Groups*** > ***Endpoint Identity Groups*** > ***RegisteredDevices***. The MAC address has been added to the database.

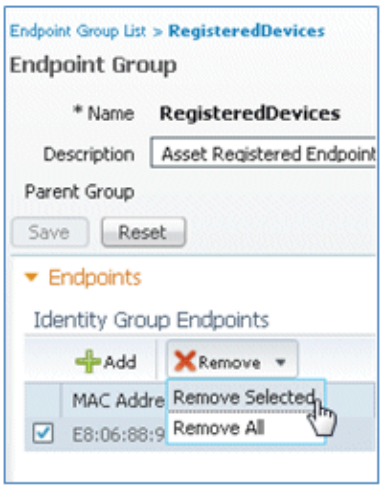


Single SSID

This section covers single SSID and describes how to connect directly to an 802.1x WLAN, provide AD username/password for PEAP authentication, provision through a guest account, and reconnect with TLS.

Complete these steps in order to provision iOS in the single SSID scenario:

1. If you are using the same iOS device, remove the endpoint from the Registered Devices.



2. On the iOS device, navigate to ***Settings*** > ***Generals*** > ***Profiles***. Remove the profiles installed in this example.



3. Click ***Remove*** in order to remove the previous profiles.





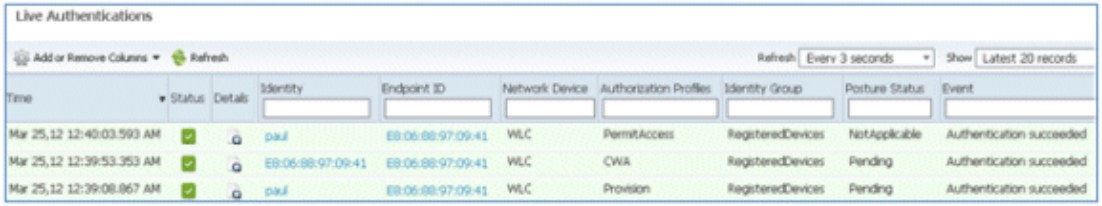
4. Connect directly to the 802.1x with the existing (cleared) device or with a new iOS device.

5. Connect to ***Dot1x***, enter a Username and Password, and click ***Join***.

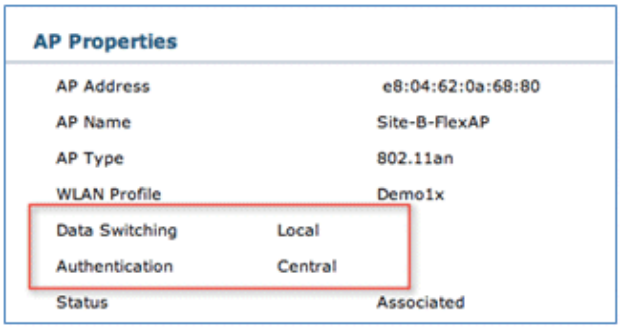


6. Repeat Steps 90 and on from the ISE Configuration section until the appropriate profiles are completely installed.

7. Navigate to ***ISE*** > ***Operations*** > ***Authentications*** in order to monitor the process. This example shows the client that is connected directly to 802.1X WLAN as it is provisioned, disconnects, and reconnects to the same WLAN with the use of TLS.



8. Navigate to ***WLC*** > ***Monitor*** > ***[Client MAC]***. In the client detail, note that the client is in the RUN state, its Data Switching is set to local, and the Authentication is Central. This is true for clients that connect to FlexConnect AP.



User Experience − Provisioning Android

Dual SSID

This section covers dual SSID and describes how to connect to the guest to be provisioned and how to connect to an 802.1x WLAN.

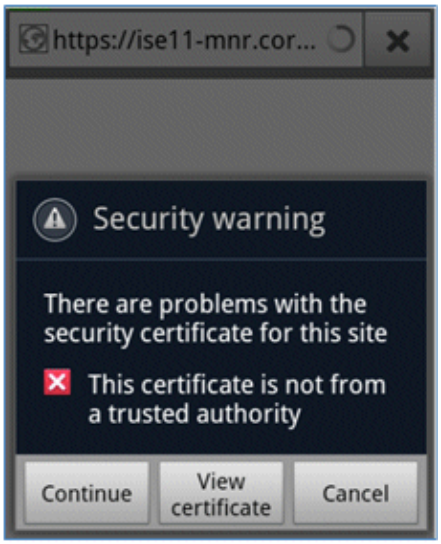
The connection process for the Android device is very similar to that for an iOS device (single or dual SSID). However, an important difference is that the Android device requires access to the Internet in order to access Google Marketplace (now Google Play) and download the supplicant agent.

Complete these steps in order to provision an Android device (such as the Samsung Galaxy in this example) in the dual SSID scenario:

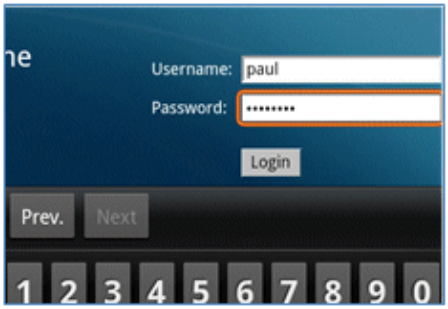
1. In the Android device, use Wi−Fi in order to connect to ***DemoCWA***, and open the guest WLAN.



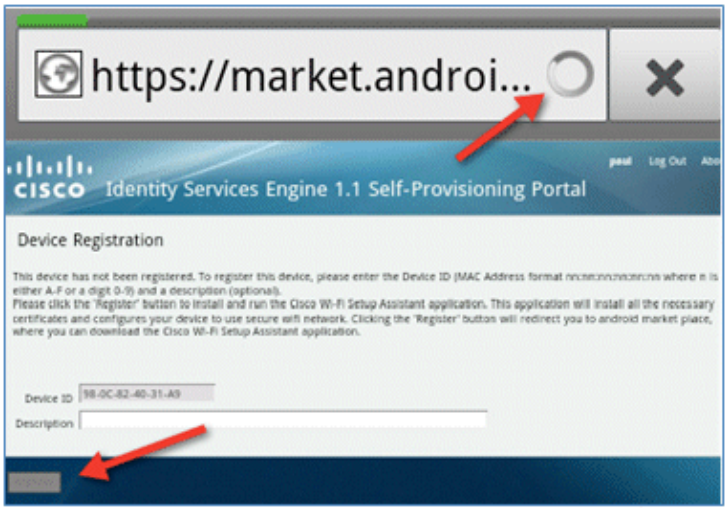
2. Accept any certificate in order to connect to the ISE.



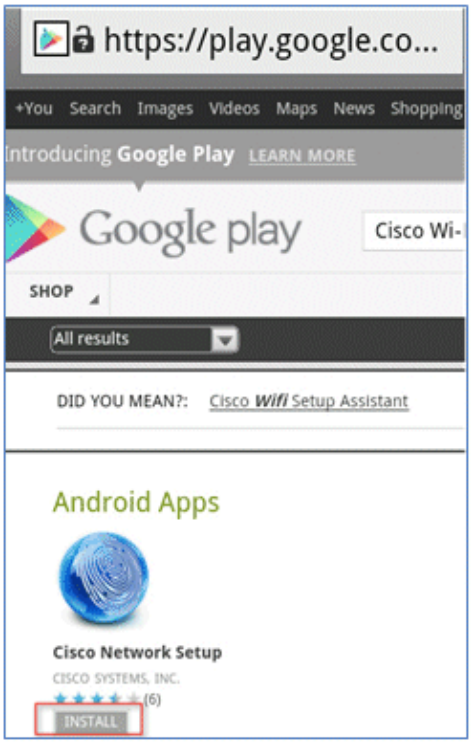
3. Enter a Username and Password at the Guest Portal in order to log in.



4. Click ***Register***. The device attempts to reach the Internet in order to access Google Marketplace. Add any additional rules to the Pre−Auth ACL (such as ACL−REDIRECT) in the controller in order to allow access to the Internet.



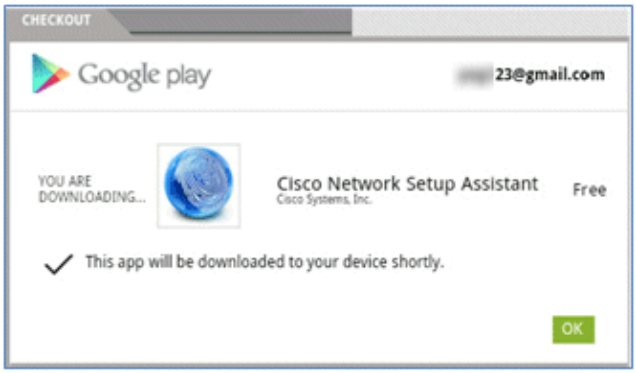
5. Google lists Cisco Network Setup as an Android App. Click ***INSTALL***.



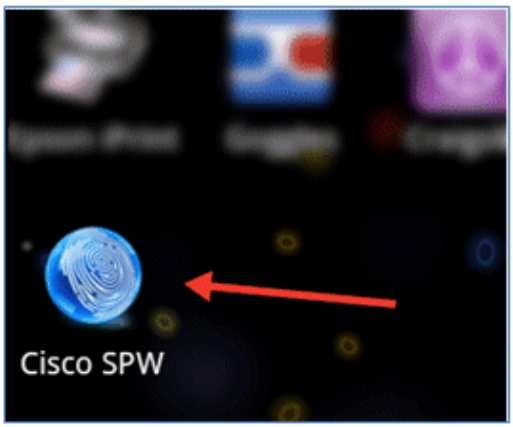
6. Sign in to Google, and click ***INSTALL***.



7. Click ***OK***.



8. On the Android device, find the installed ***Cisco SPW*** app, and open it.



9. Make sure that you are still logged in to the Guest Portal from your Android device.

10. Click ***Start*** in order to start the Wi−Fi Setup Assistant.



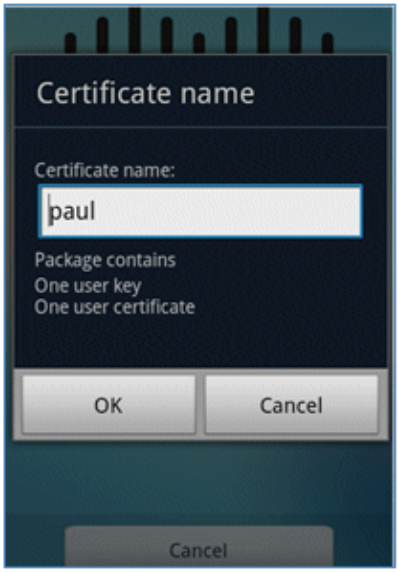
11. The Cisco SPW begins to install certificates.



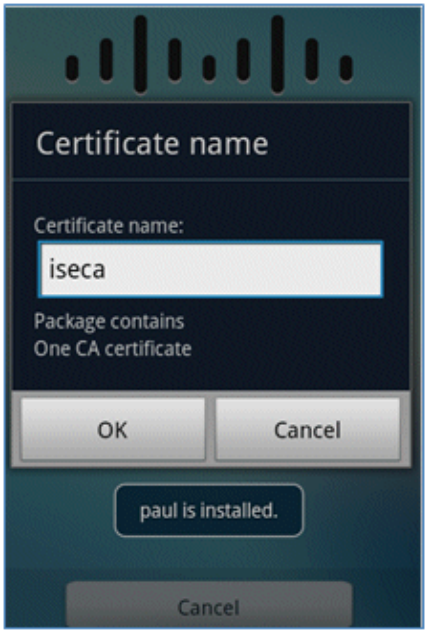
12. When prompted, set a password for credential storage.



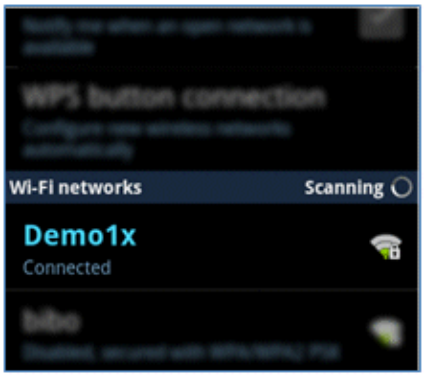
13. The Cisco SPW returns with a certificate name, which contains the user key and user certificate. Click ***OK*** in order to confirm.



14. Cisco SPW continues and prompts for another certificate name, which contains the CA certificate. Enter the name ***iseca*** (in this example), then click ***OK*** in order to continue.



15. The Android device is now connected.

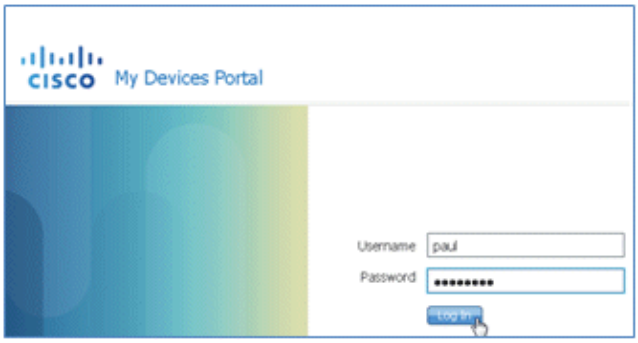


My Devices Portal

My Devices Portal allows users to blacklist previously registered devices in the event a device is lost or stolen. It also allows users to re−enlist if needed.

Complete these steps in order to blacklist a device:

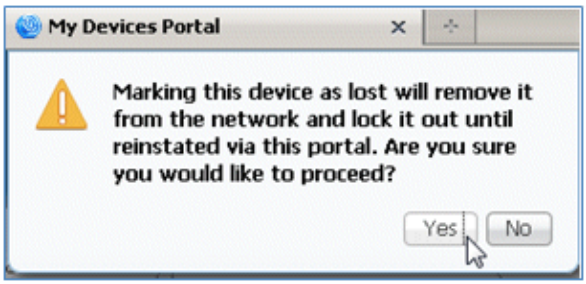
1. In order to log in to My Devices Portal, open a browser, connect to https://ise−server:8443/mydevices (note the port number 8443), and log in with an AD account.



2. Locate the device under Device ID, and click ***Lost?*** in order to initiate blacklisting of a device.



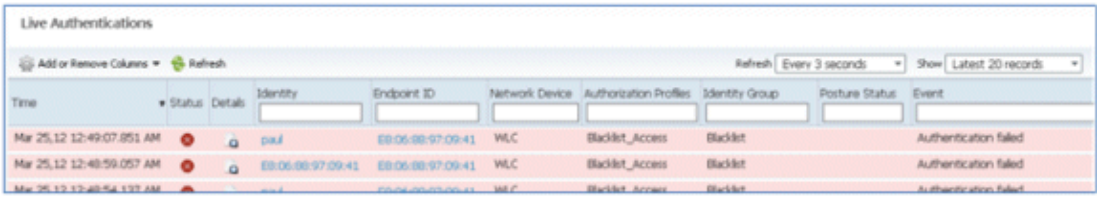
3. When the ISE prompts a warning, click ***Yes*** in order to proceed.



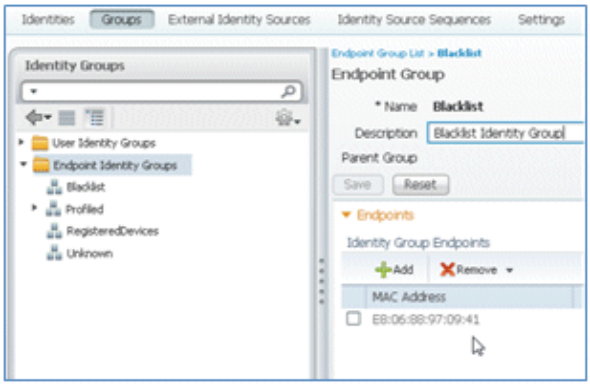
4. ISE confirms that the device is marked as ***lost***.



5. Any attempt to connect to the network with the previously registered device is now blocked, even if there is a valid certificate installed. This is an example of a blacklisted device that fails authentication:



6. An administrator can navigate to ***ISE*** > ***Administration*** > ***Identity Management*** > ***Groups***, click ***Endpoint Identity Groups*** > ***Blacklist***, and see the device is blacklisted.

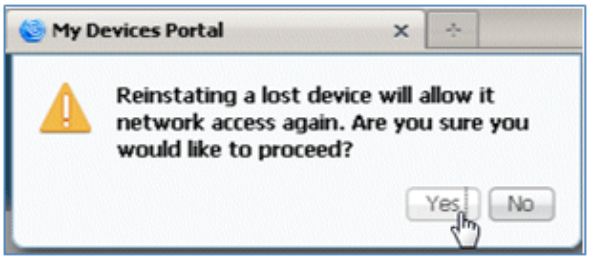


Complete these steps in order to reinstate a blacklisted device:

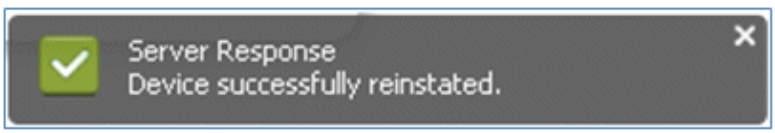
1. From the My Devices Portal, click ***Reinstate*** for that device.



2. When ISE prompts a warning, click ***Yes*** in order to proceed.



3. ISE confirms that the device has been successfully reinstated. Connect the reinstated device to the network in order to test that the device will now be permitted.

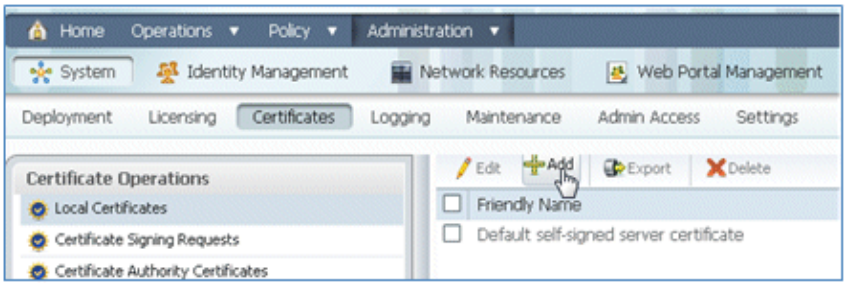


Reference − Certificates

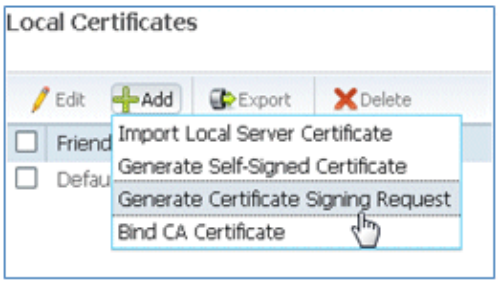
ISE not only requires a valid CA root certificate, but also needs a valid certificate signed by CA.

Complete these steps in order to add, bind, and import new trusted CA certificate:

1. Navigate to ***ISE*** > ***Administration*** > ***System*** > ***Certificates***, click ***Local Certificates***, and click ***Add***.



2. Select ***Generate Certificate Signing Request*** (CSR).



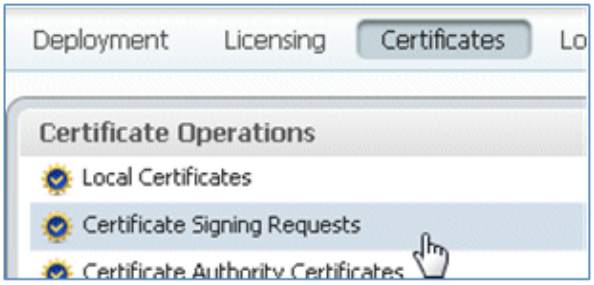
3. Enter the Certificate Subject ***CN=***<*ISE−SERVER hostname.FQDN*>. For the other fields, you can use the default or the values required by your CA setup. Click ***Submit***.



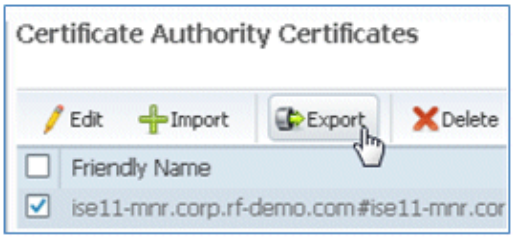
4. ISE verifies that the CSR was generated.



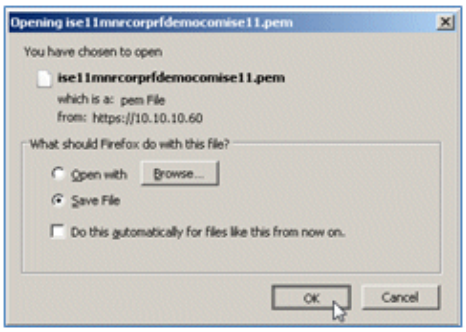
5. In order to access the CSR, click the ***Certificate Signing Requests*** operations.



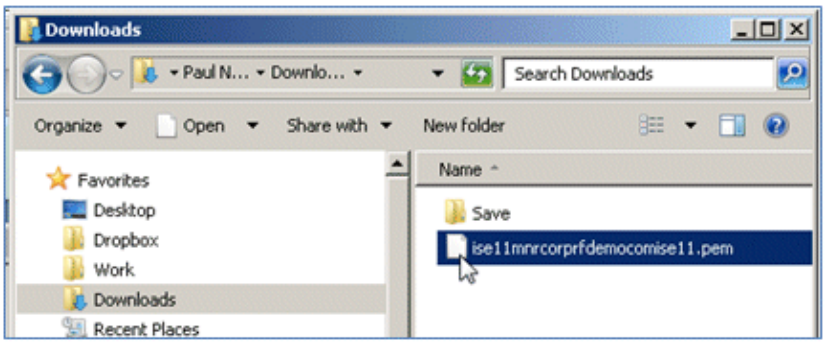
6. Select the CSR recently created, then click ***Export***.



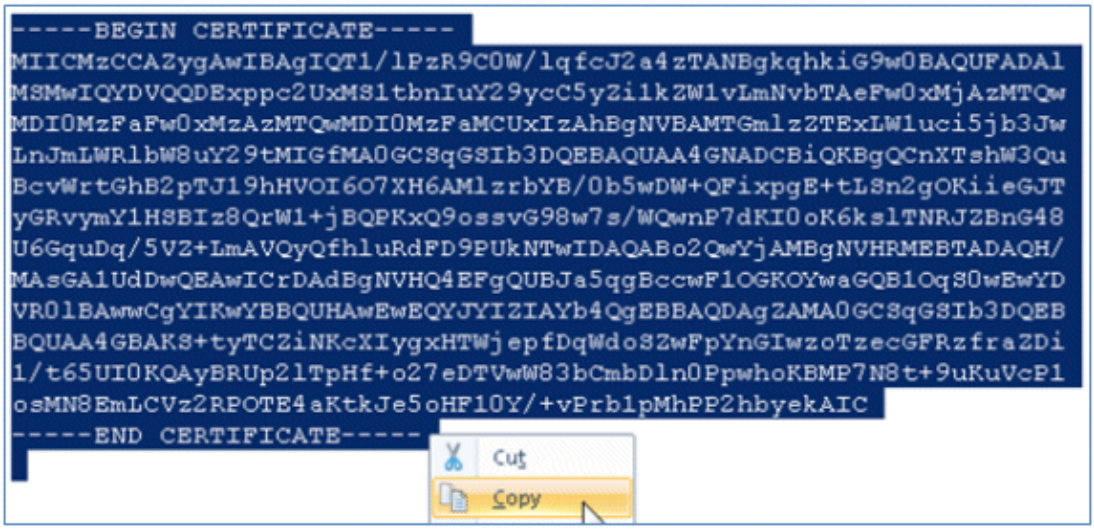
7. ISE exports the CSR to a .pem file. Click ***Save File***, then click ***OK*** in order to save the file to the local machine.



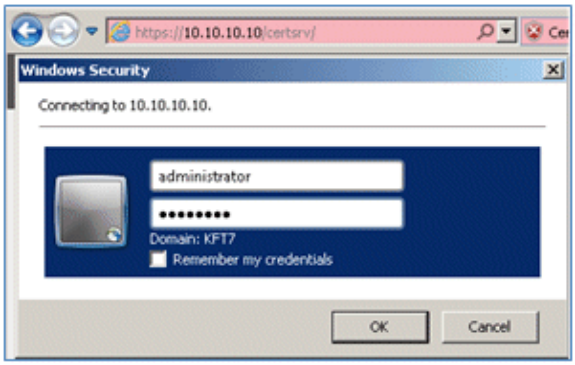
8. Locate and open the ISE certificate file with a text editor.



9. Copy the entire content of the certificate.



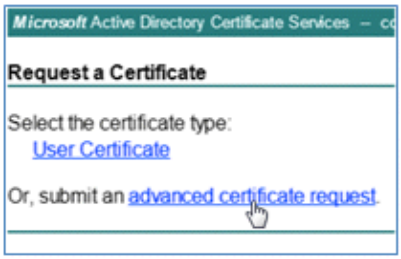
10. Connect to the CA server, and log in with an administrator account. The server is a Microsoft 2008 CA at https://10.10.10.10/certsrv (in this example).



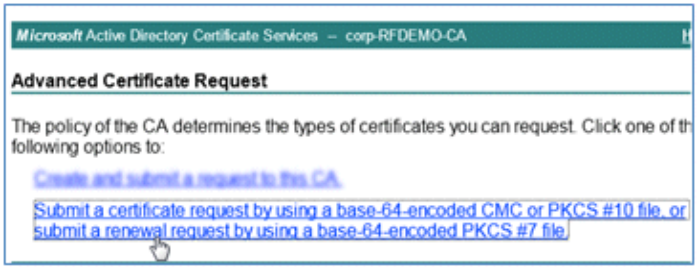
11. Click ***Request a certificate***.



12. Click ***advanced certificate request***.



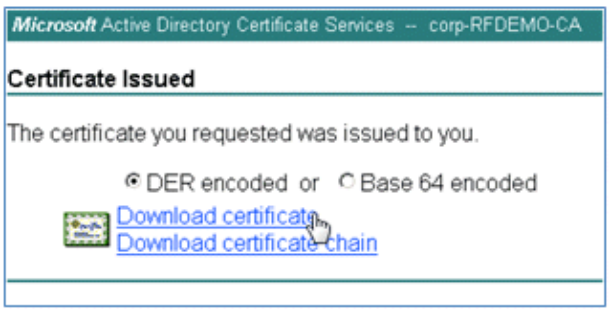
13. Click the second option in order to ***Submit a certificate request by using a base−64−encoded CMC or ...*** .



14. Paste the content from the ISE certificate file (.pem) into the Saved Request field, ensure the Certificate Template is ***Web Server***, and click ***Submit***.



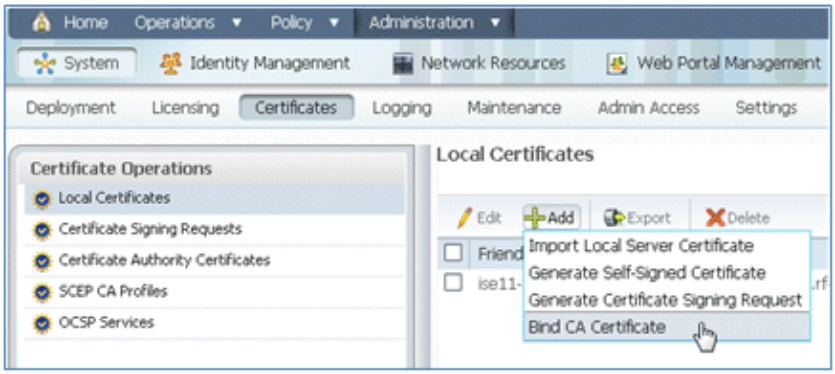
15. Click ***Download certificate***.



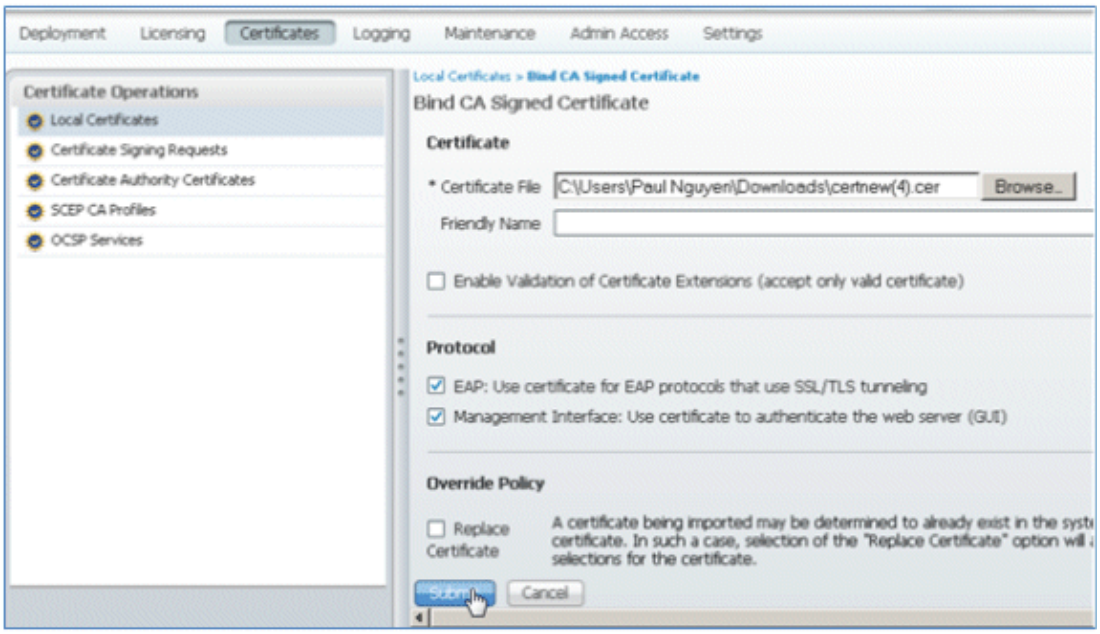
16. Save the certnew.cer file; it will be used later in order to bind with the ISE.



17. From ISE ***Certificates***, navigate to ***Local Certificates***, and click ***Add*** > ***Bind CA Certificate***.



18. Browse to the certificate that was saved to the local machine in the previous step, enable both the ***EAP*** and ***Management Interface*** protocols (boxes are checked), and click ***Submit***. ISE may take several minutes or more in order to restart services.



19. Return to the landing page of the CA (https://CA/certsrv/), and click ***Download a CA certificate, certificate chain, or CRL***.



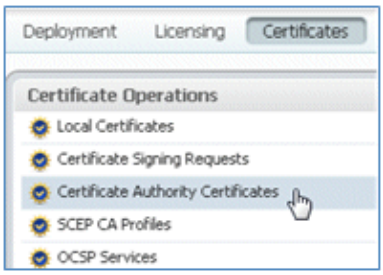
20. Click ***Download CA certificate***.



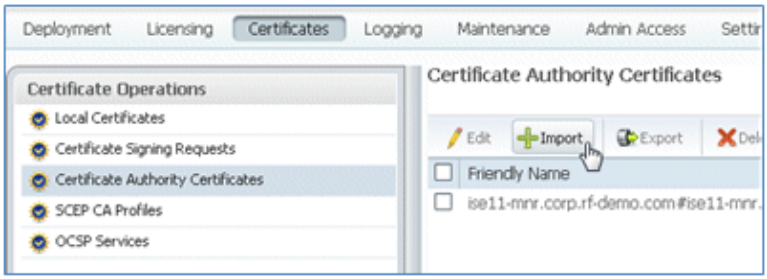
21. ***Save*** the file to the local machine.



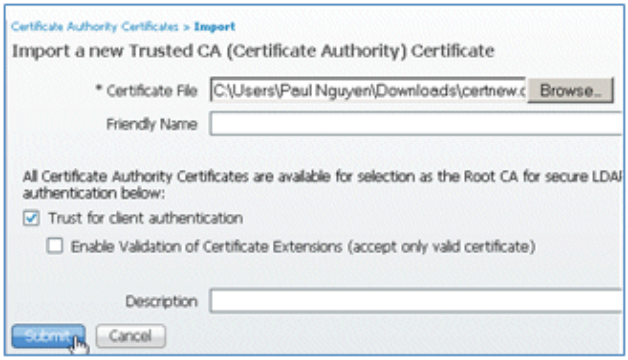
22. With the ISE server online, go to ***Certificates***, and click ***Certificate Authority Certificates***.



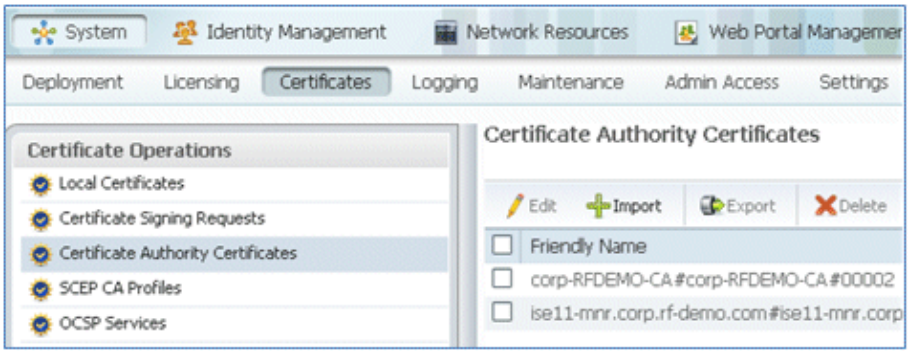
23. Click ***Import***.



24. Browse for the CA certificate, enable ***Trust for client authentication*** (box is checked), and click ***Submit***.



25. Confirm that the new trusted CA certificate is added.



Related Information

- ***Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4***
- ***Cisco 2000 Series Wireless LAN Controllers***
- ***Cisco 4400 Series Wireless LAN Controllers***
- ***Cisco Aironet 3500 Series***
- ***Flex 7500 Wireless Branch Controller Deployment Guide***
- ***Bring Your Own Device − Unified Device Authentication and Consistent Access Experience***
- ***Wireless BYOD with Identity Services Engine***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Sep 12, 2013 Document ID: 113606