Guide

Cisco TrustSec® How-To Guide: AnyConnect Network Access Manager Enterprise Connection Enforcement

For further information, questions and comments please contact ccbu-pricing@cisco.com

Contents

Introduction

Executive Summary

Employees connect to non-corporate WiFi access points while sitting at their desks or in a conference room, even though the corporate WiFi network is in range and working fine. Some employees connect to a third-party WiFi hotspot to check their personal email or shop on the Internet during normal business hours. Others try to gain access to a competitor's network one floor above, or to a nearby apartment complex. Still others access the guest network because it might have somewhat better performance. Employees should be connecting their corporate laptops to the corporate network, not to these other networks.

Blacklisting is the first thought we think as far as keeping employees from wandering onto other peoples' networks or their own guest networks. While this is a great idea for preventing employees from accessing the guest network, it can have some unintended consequences.

Employees need to access their home networks and WiFi hotspots so they can use the VPN to access the corporate network when they are traveling or working from home. So, while we would like to blacklist Linksys® to prevent employees from accessing a network at the apartment complex across the street during the day, we need to let them access their own Linksys home network at night.

Blacklisting also ends up being site specific. Blacklisting one competitor that is in the same office tower in New York does not apply in Paris or Tokyo, where there might be different competitors. Blacklisting is easy to deploy if your business has one location. It is nearly impossible to manage if you are a multinational corporation with hundreds or thousands of sites around the world.

Cisco® approached the problem focusing on the corporate WiFi network rather than eliminating non-corporate networks. When the corporate network is in range, there is no need to connect to any other network. When the corporate network is not in range, employees are free to connect to other networks.

Enterprise Connection Enforcement gives IT administrators the ability to select one or more WiFi networks as corporate networks. When any or all of those networks are in range, employees can connect to any of the specified corporate WiFi networks, but employees are prevented from connecting to any third party networks.

Cisco Identity Services Engine (ISE) will provide the back-end RADIUS functions and provide policy control for 802.1X authentication. In this document, EAP-FAST will be used as the authentication method.

About this Document

This document illustrates Cisco AnyConnect® Network Access Manager's Enterprise Connection Enforcement feature. It automatically connects to the corporate network designated by the administrator- defined corporate service set identifiers (SSIDs) in the AnyConnect Network Access Manager profile. If any end users connect to non-corporate access points, they will be denied.

When a user connects to a wired corporate network and obtains an internal IP address, the wireless connection will be dropped. EAP-FAST (MSCHAPv2) will be used as the authentication method for wireless and configured within the AnyConnect Network Access Manager profile by the administrator. Both machine and user connection types will also be defined. The ISE server will be configured to use Microsoft AD for machine and user validation, EAP-FAST (MSCHAPv2) for 802.1X authentication, and for creating the Authentication and Authorization policies. Wireless controller configuration information is also included.

In this document, the wired connection will be configured for open authentication to simulate a wired corporate connection.

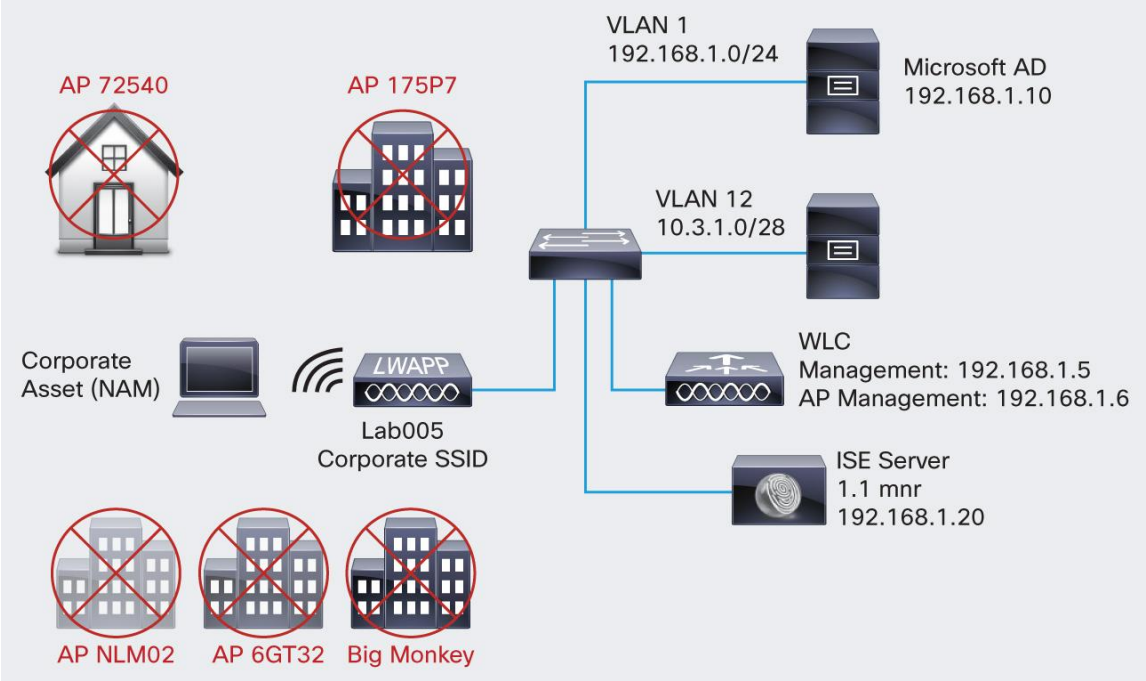
Scenario Overview

The AnyConnect Network Access Manager profile will contain the EAP-FAST authentication method, and the corporate wireless network designated SSID, which will be lab005. The user will automatically to connect to the corporate wireless network. When the user tries to connect to non-corporate access points, he or she will be denied.

When the user connects to the wired network, he or she will be automatically disconnected from the wireless network.

ISE will be used as the back-end RADIUS server, and the successful authentication logs will be reviewed.

Architecture



Software and Hardware Requirements

Client:

- Laptop or desktop computer with an Ethernet NIC or WiFi NIC and one of the following operating systems:
  - Windows 7 SP1 x 86 (32-bit) and x64 (64-bit)
  - Windows Vista SP2 x86 and x64
  - Windows XP SP3 x86
- Windows Server 2003 SP2 x86
- Cisco AnyConnect 3.1 or greater with the Network Access Manager installed
- Cisco AnyConnect 3.1 or greater Profile Editor

Authentication Server:

- Cisco ISE System 1.1.1 or greater

Network Infrastructure:

- Ethernet switch or WiFi access point configured for 802.1X

Technology Primer

The Enterprise Connection Enforcement feature will only work with WiFi networks, as well as with administratively defined networks. User-created network configurations will be ignored.

The AnyConnect Network Access Manager will initiate scan requests periodically and retrieve the scan-list to see if any corporate networks are in range and probe for hidden SSIDs on Windows 7 hosts. On Windows XP hosts, probing for hidden SSIDs is not possible and will be non-hidden.

In the event that no wired connections are available, a connection to wireless corporate networks will be allowed, and a connection to non-corporate networks will be denied.

Each corporate network shall be tagged by AnyConnect Network Access Manager and all in-range corporate networks are added to a list of available networks for matching, alternatively non-corporate networks are removed from the list of available networks for matching.

The AnyConnect Network Access Manager will start matching one corporate network to one of the adapters:

- The connection mode is automatic, the connection attempt will be made to corporate networks in the list of available networks for matching one by one until one network is successfully connected.
- If all networks in the list of available networks for matching are tried, but no successful connection is made, the AnyConnect Network Access Manager will start over again from the beginning of the list, this is not admin configurable. The AnyConnect Network Access Manager will not fall back to non-corporate networks.

There are no limitations imposed on the number of network profiles which are designated as corporate networks, and whose SSIDs are configured as non-broadcasting (for example, hidden). However, due to technical limitations in this release of the AnyConnect Network Access Manager, only one hidden SSID can be probed at a time.

Therefore, after reading the profiles sequentially from the configuration, the AnyConnect Network Access Manager will choose the first corporate and hidden network and use its SSID for probing purposes. The remaining corporate networks will be treated as broadcasting Wi-Fi networks for detection of hidden SSIDs, even though they are configured as hidden.

Design Parameters

EAP Methods

The 802.1x authentication framework has been incorporated as part of the 802.3 (Wired Security) and 802.11 (Wireless Security) standard to enable layer-2 based authentication, authorization, and accounting functions in an 802.3 wired network. Today, there are several EAP protocols available for deployment in both wired and wireless networks. The most common EAP protocols are LEAP, PEAP, EAP-FAST, and EAP-TLS. In this document EAP-FAST will be used for 802.1X authentication.

EAP-FAST: EAP-FAST (Flexible Authentication using Secure Tunneling) is defined in RFC 4851 and was developed by Cisco. The protocol was designed to address the weaknesses of LEAP while preserving the lightweight implementation. Instead of using a certificate, mutual authentication is achieved by means of a Protected Access Credential (PAC). PAC files details are covered in the Encryption section below.

EAP-FAST has three phases:

- **Phase 0:** An optional phase in which the PAC, can be provisioned manually or dynamically (used in this case, with ISE server)
- **Phase 1:** In this phase, the client and the authentication server uses the PAC to establish TLS tunnel.
- **Phase 2:** In this phase, the client credentials are exchanged inside the encrypted tunnel, using an inner method for authentication.

Identity Source and Database

When deploying in a wired/wireless network and seeking an authentication protocol, it is common to use an existing database of user and machine authentication credentials. Typical databases are Windows Active Directory (AD), LDAP, or a one-time password (OTP) database (for example, RSA SecureID). All of these databases are compatible with the EAP-FAST protocol.

When planning for deployment, there are compatibility requirements, such as EAP Chaining, which requires AD for machine and user validation. For the purpose of this document, AD will be used as the database. EAP Chaining will be enabled in the EAP-FAST protocol selection on the ISE node.

Encryption

EAP-TLS is a strong authentication method, requiring server and client-based X.509 certificates that also need PKI for certificate deployment. Another strong authentication method, EAP-FAST, does not require client side certificates for mutual authentication. Instead, Protected Access Credential (PAC) files are used, which can be provisioned either manually or automatically.

In this document, the PAC files are automatically provisioned from the ISE server to the client if the client does not contain as existing PAC file. Anonymous PAC provisioning uses EAP-TLS with an anonymous key agreement protocol to establish a highly secure TLS tunnel. In addition, MSCHAPv2 is used to authenticate the client and prevent early MITM attack detection.

Authenticated In-Band PAC provisioning uses TLS server-side authentication, requiring server certificates for establishing the highly secure tunnel. Since unauthenticated PAC provisioning does not require server side validation, it has some security risks, such as allowing rogue authentications to mount a dictionary attack. In this document, the AnyConnect Network Access Manager configuration profile will be configured for unauthenticated PAC provisioning for testing purposes only.

A PAC file is a security credential generated by the ISE server that holds information specific to the client. These PAC files, machine tunnel (also known as machine authentication) are used to establish the highly secure TLS tunnel, and user authorization for validation of user credentials during inner method authentication exchanges. They also prove that the client and machine were authenticated and the current authentication process can be optimized and bypassed. PAC type 4 has been added to support EAP Chaining.

Configuring the Wireless LAN Controller

This configuration requires the following steps:

Configure the Wireless LAN Controller (WLC) with the details of the Authentication Server

Configure WLAN parameters

Configure the dynamic interfaces (VLANs)

Configuring the WLC with the Details of the Authentication Server

The WLC needs to be configured to forward the machine and user credentials to the ISE server. The ISE server then validates these credentials (using the configured Windows database) and provides access to the wireless clients. Based on the initial WLC script install, RADIUS was configured and the values will be prefilled.

Step 1. From the controller GUI, click **Security->Radius ->Authentication->New**.

Step 2. Enter the **IP address of the RADIUS server** and the **Shared Secret** key used between the RADIUS server and the WLC.

Note: Values will be prefilled if RADIUS is configured as part of WLC installation script

The **Network User** and **Management** check boxes determine if the RADIUS-based authentication applies for users (for example, WLAN clients) and management (for example, administrative users).

In this example, the ISE is used as the RADIUS server with the IP address of 192.168.1.20 and the communication port as 1645.

Figure 1. RADIUS Configuration

Configure WLAN Parameters

Configure the WLAN (the WLAN specifies a SSID and associated security parameters) which the clients use to connect to the wireless network. When you configured the basic parameters for the WLC using the configuration wizard, you also configured the initial SSID for the WLAN Controller. You can use the SSID for the WLAN or create a new SSID.

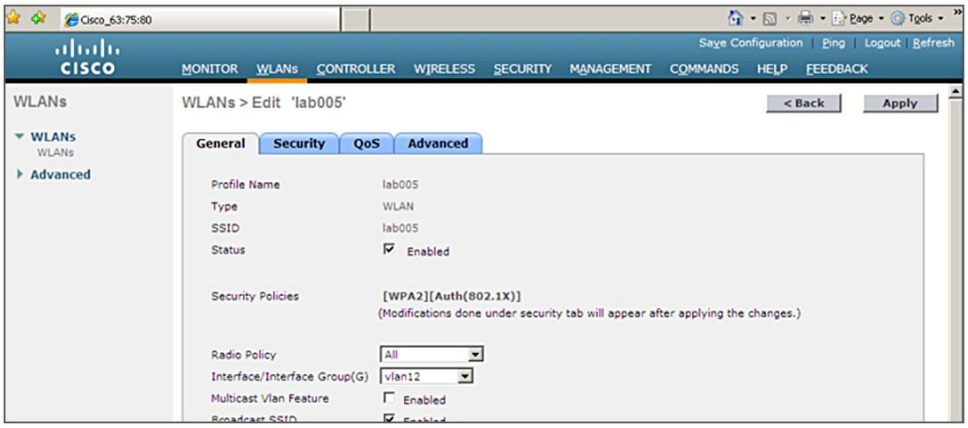
Step 1. From the GUI, **select ->WLANS**, to display the WLANs page. This page lists the WLANs that are created by the initial script controller.

Figure 2. WLAN Parameters

Step 2. From the GUI, select**->WLANs->WLAN ID 1**. In this page, you can define various parameters specific to this WLAN, including General Policies, RADIUS Servers, Security Policies, and 802.1X parameters. Notice that **Broadcast SSID** and **Status** are enabled.

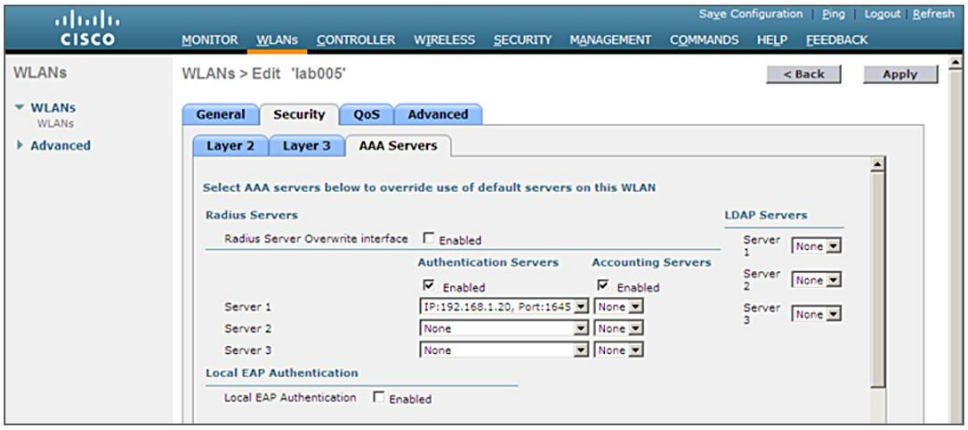
Note that although non-broadcast of SSID is not considered a broadcast mechanism, it is recommended to disable SSID broadcast to discourage casual WLAN observers and inadvertent client association attempts. You can also elect to create new WLANs by selecting **Create New-Go**

Figure 3. WLAN Screen



Step 3. From the GUI, select**->WLANs->WLAN ID 1->Security->AAA Servers** to select the configured ISE server.

Figure 4. RADIUS Server Selection



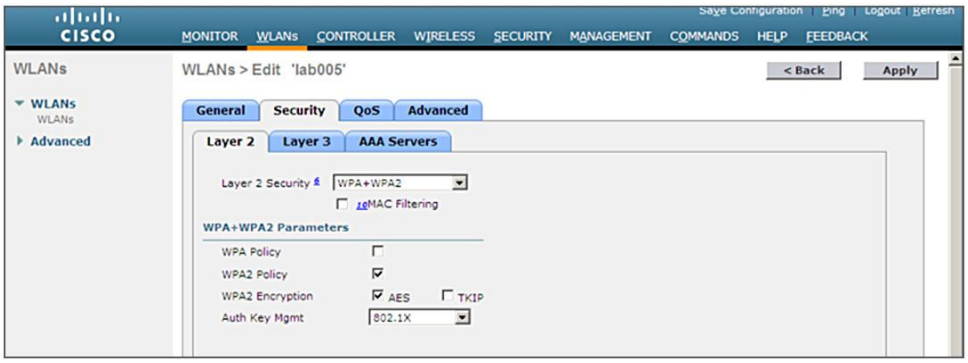
Step 4. Under Security Policies, configure **L2 Security for WPA+WPA2**. Also select the appropriate **encryption types** under WPA+WPA2 Parameters. Although network access manager supports all of these encryption types, the settings chosen here depend on the client NIC card capabilities.

`In this example, WPA2 Encryption` **`AES`** `was used.`

Note: Enabling WPA encryption permits the flexibility to support older WPA clients, as well as newer WPA2-capable clients.

Step 5. Click **Apply**

Figure 5. L2 Security



Configure Dynamic Interfaces (VLANS)

In this document, the wireless client will be placed in VLAN 12 after authentication. Note the VLAN ID specified under the Tunnel-Private-Group ID attribute of the RADIUS server must also exist in the WLC.

The end user is specified with the Tunnel-Private-Group ID of 12 VLAN=12) on the RADIUS server. You can see the same dynamic interface (VLAN=12) configured in the WLC.

Step 1. From the controller GUI, click **Controller->Interfaces**.

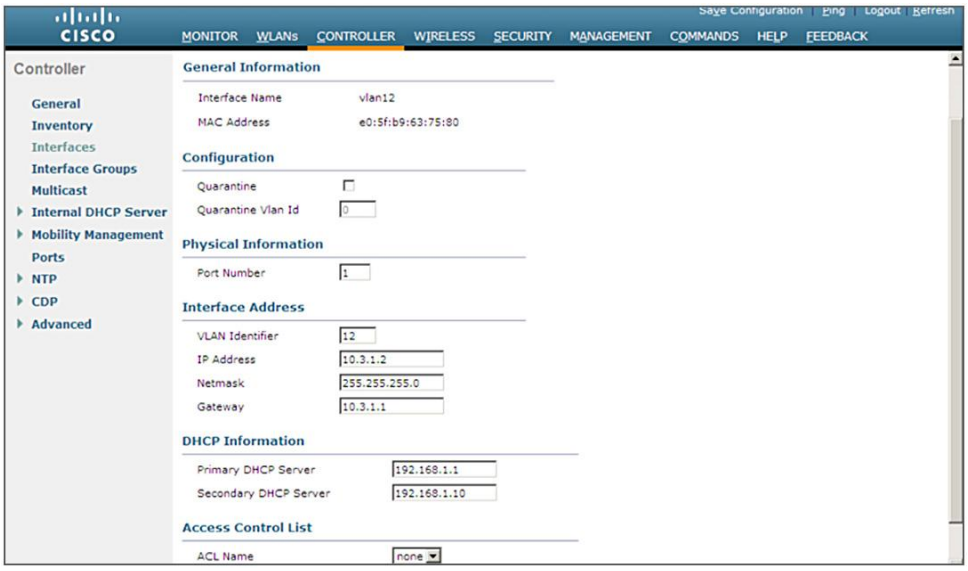
Step 2. Enter **vlan12** for both the Interface Name and 12 the VLAN id.

Figure 6. VLAN Interface Configuration

Step 3. Click **Apply** on this window.

Step 4. Enter the IP Address and default Gateway of this Network Access Manager interface.

Figure 7. Enter IP and Gateway address



Step 5. Click **Apply**.

Configure WLANs (SSID)

This procedure explains how to configure the WLANs in the WLC.

Step 1. From the controller GUI, select->**WLANs->New** to create a new WLAN.

Step 2. Enter the **WLAN ID and WLAN SSID information**.

`In this example, VLAN12 was used for both.`

Figure 8. WLAN Configuration

Step 3. Click **Apply**.

Figure 9. VLAN Information

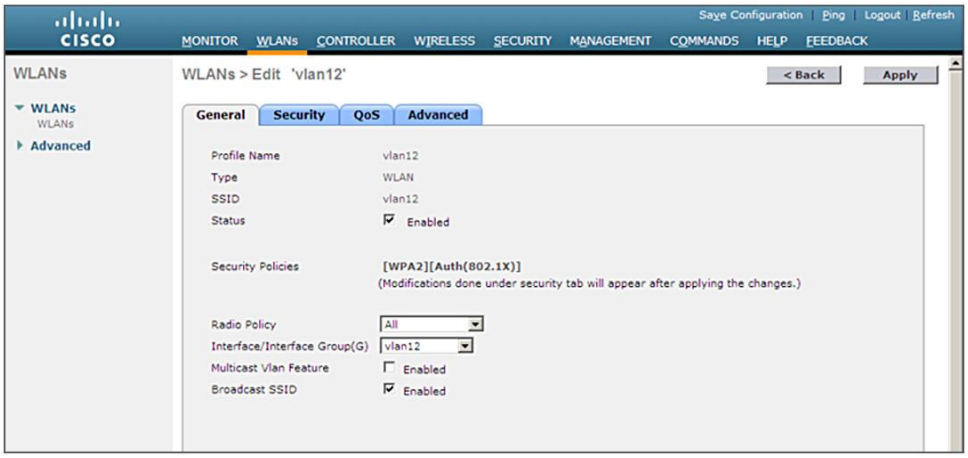
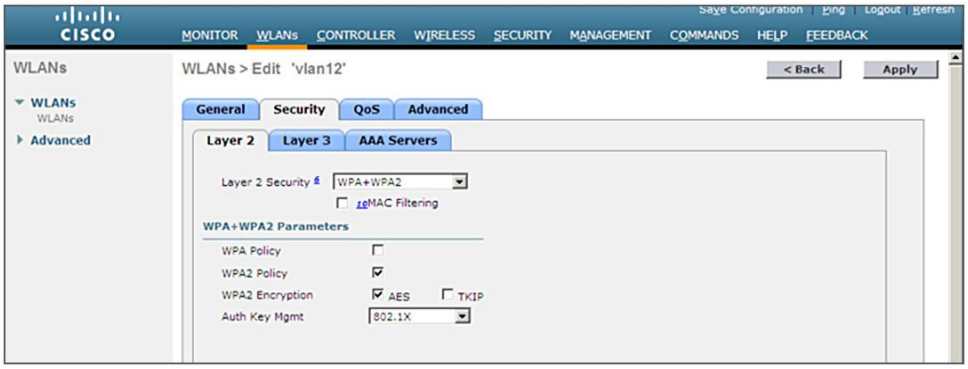


Figure 10. VLAN Information



Normally, in a wireless LAN controller, each WLAN is mapped to a specific VLAN (SSID) so that a particular user that belongs to that WLAN is put into the specific VLAN mapped. This mapping is normally done under the Interface Name field of the WLAN SSID window.

Step 4. From the GUI, select**->WLANS->WLAN ID->**and change the interface name from **Management to VLAN 12->Apply**.

Figure 11. Interface Name

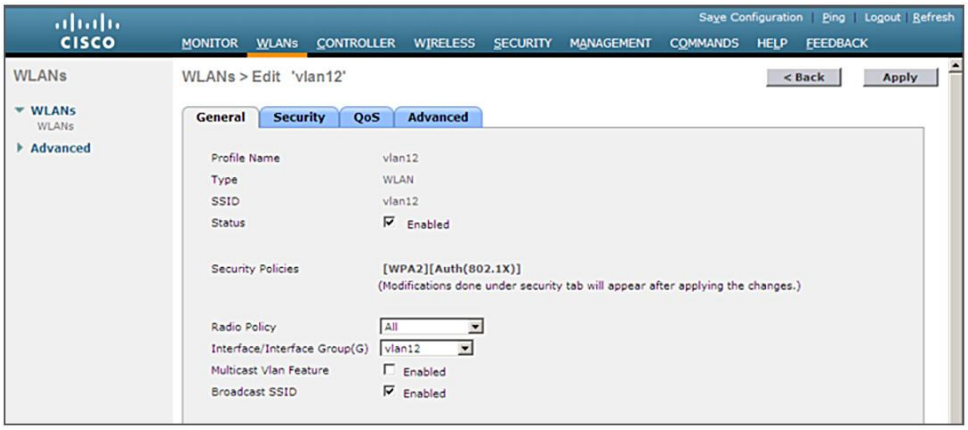
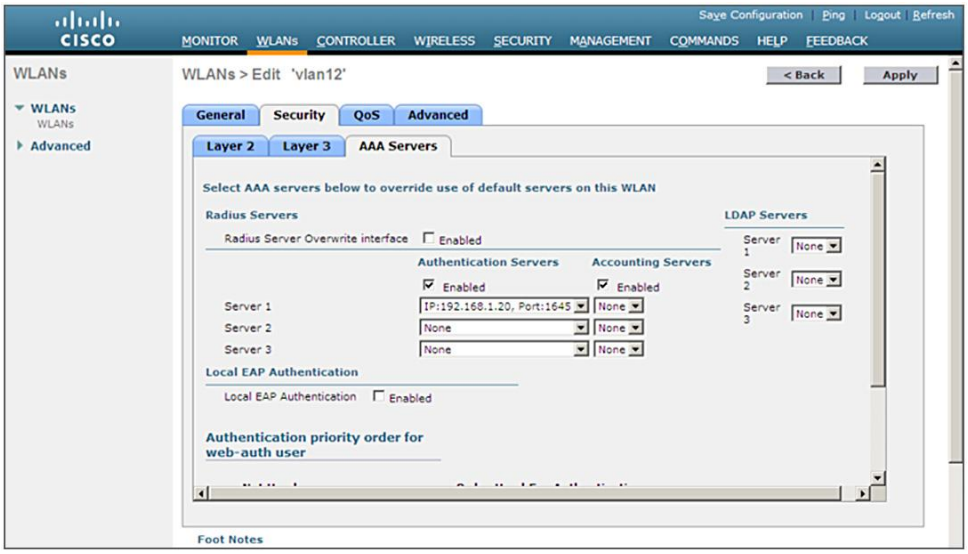


Figure 12. RADIUS server configuration for VLAN 12



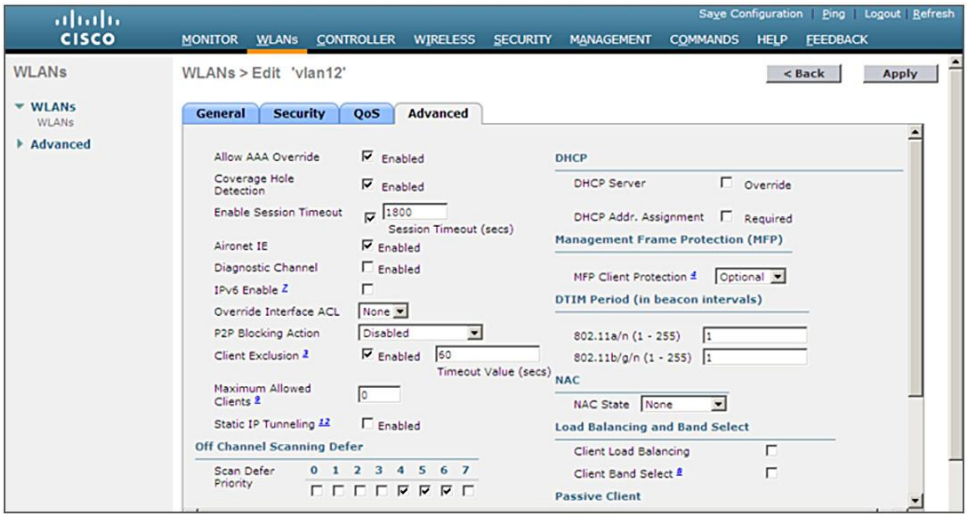
In the example provided, the RADIUS server assigns a wireless client to a specific VLAN upon successful authentication. The WLANs need not be mapped to a specific dynamic interface on the WLC. Even though the WLAN to dynamic interface mapping is done on the WLC, the RADIUS server overrides this mapping and assigns the user that comes through that WLAN to the VLAN specified under the user **Tunnel-Group-Private-ID** field in the RADIUS server.

Step 5. Check the **Allow AAA Override** check box to override the WLC configurations by the RADIUS server.

Step 6. Enable the **Allow AAA Override** in the controller for each WLAN (SSID) configured.

Step 7. From the GUI, select **->WLANS->WLAN ID->Advanced**.

Figure 13. VLAN 12 Advanced Configuration



When AAA Override is enabled, and a client has AAA and controller WLAN authentication parameters that conflict, client authentication is performed by the AAA (RADIUS) server. As part of this authentication, the operating system moves clients to a VLAN returned by the AAA server. This is predefined in the controller interface configuration

Step 8. Select**->Save** Configuration.

Configuring the Cisco Identity Services Engine

This section describes how to configure the Cisco Identity Services Engine (ISE), starting with adding the WLC as a network device. Active Directory will be added as en external Identity Source, and an Authentication and Authorization Policy will be created.

Add Networking Devices to ISE

Add WLC controller to ISE and provide a shared secret under Authentication Settings.

Step 1. Select->**Network Resources-Network Devices->Administration->Add**.

Step 2. Enter the **name of the WLC**

`In this example, WLC was used.`

Step 3. Enter the **IPAddress**.

`In this example, 192.168.1.5 was used.`

Step 4. Click on **Authentication Settings** and enter the **shared secret**.

Figure 14. Network Device Name and IP Address Configuration

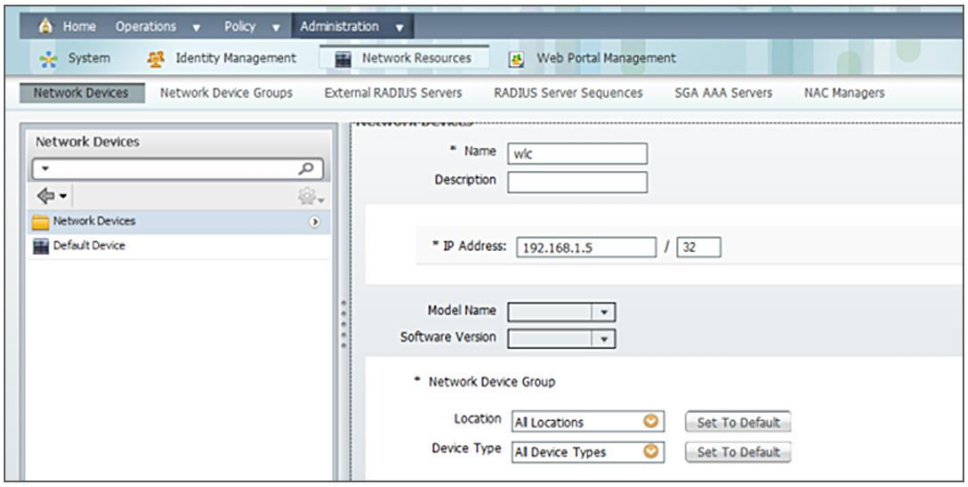
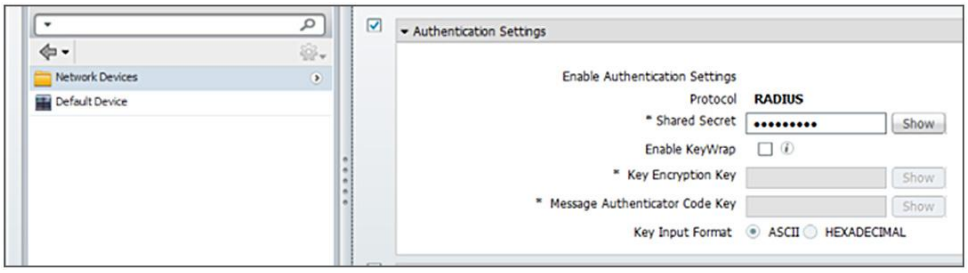


Figure 15. Authentication Settings



Step 5. Click on **Submit**.

Add Microsoft Active Directory as the External Identity Store

Machine and user credentials will be validated against the AD domain and identified as an external identity store.

Step 1. Select->**Administration->Identity Management->External Identity Sources->Active Directory**.

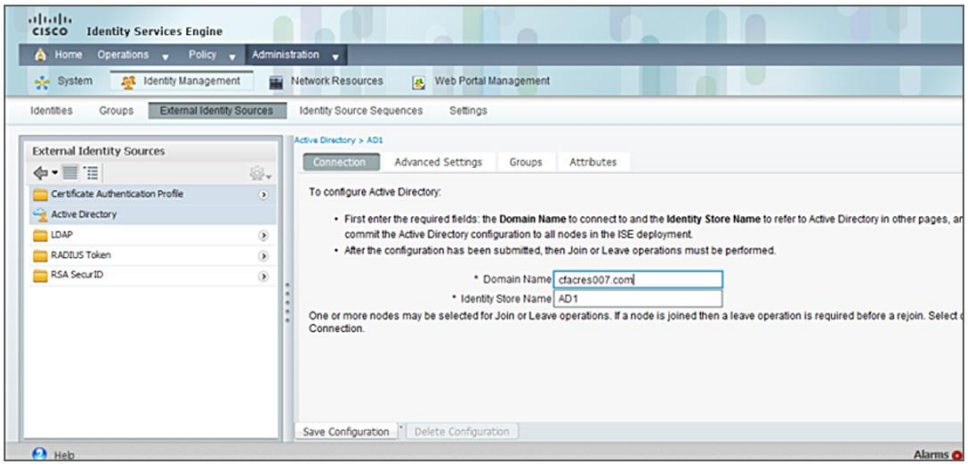
Step 2. Enter **Domain Name**.

`In this example, cfacres007.com was used.`

Step 3. Enter the **Identity Store Name**.

`In this example, the default "AD1" was used.`

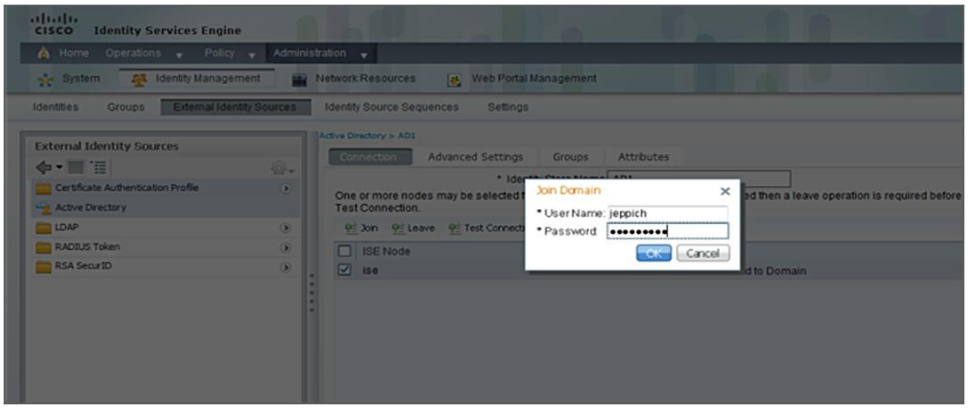
Figure 16. Active Directory Configuration)



Step 4. Click on **Save Configuration**.

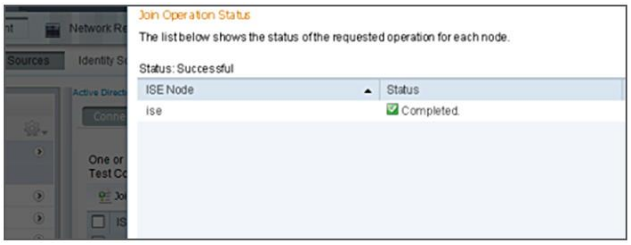
Step 5. Select the **ISE node, ISE**, and **Join Domain**.

Figure 17. Joining the Domain



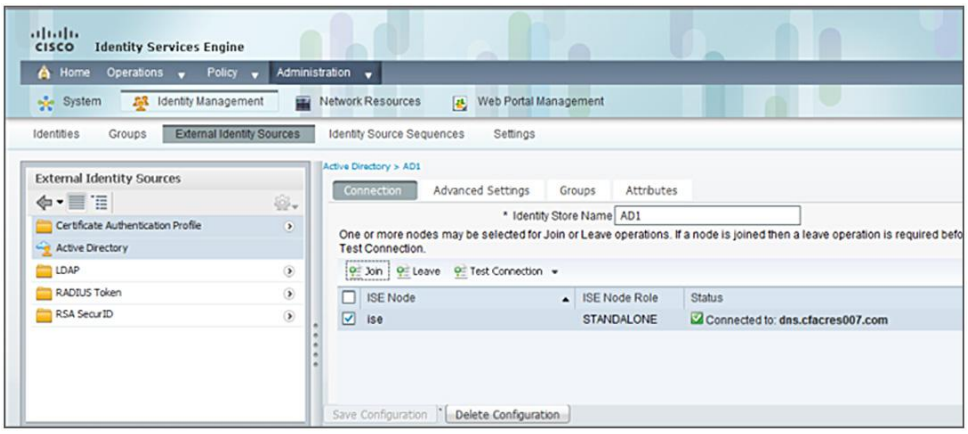
Step 6. Click on **OK**. You should see a message that the node was joined successfully.

Figure 18. Join Operation Successful



You should now see that ISE is successfully connected to the domain in Figure 5.

Figure 19. ISE successfully connected to domain



Configure Active Directory Groups

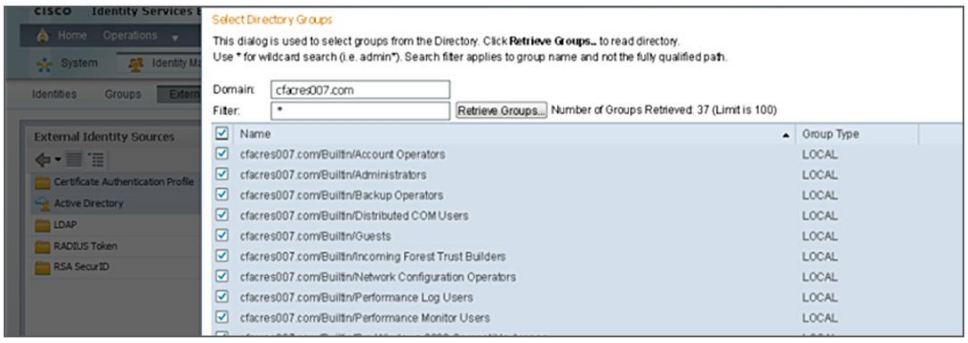
Step 1. Select->**Administrative->Identity Management->External Identity-Sources-Active Directory**.

Step 2. Select->**Groups->Add.**

Step 3. Select any **active directory groups** that you will use for your deployment.

Note: If you leave the "*" by default, this will display all the AD groups (up to 100).

Figure 20. Retrieved Groups from Active Directory



Step 4. Click **OK**, and then **Save Configuration**.

Define Identity Store Source

Identity Source Sequences define the order in which the Cisco ISE will look for the validation of user and machine credentials in the different databases, and will be configured to search in Active Directory.

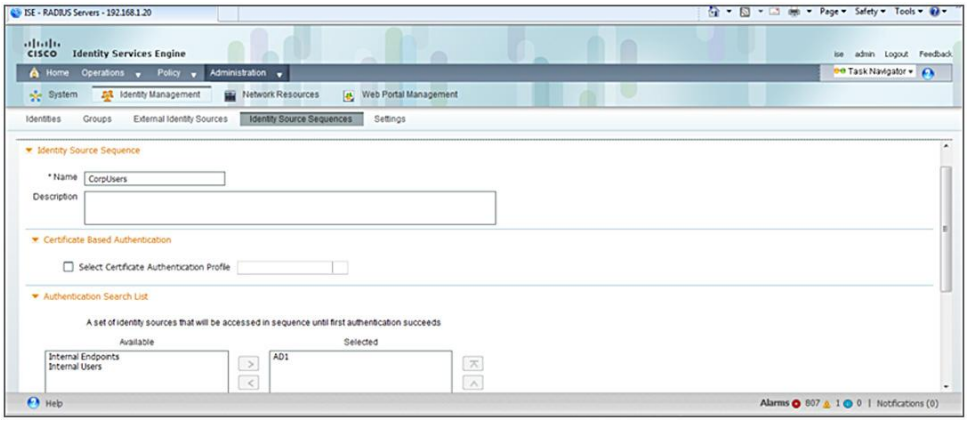
Step 1. Select->**Administration->Identity Management->Identity Source Sequence->Add**.

Step 2. Enter name of **Identity Source**.

```
In this case, CorpUsers was used
```

Step 3. Under Authentication Search List, select **AD1** and click on **>**. This will show up under Selected.

Figure 21. Identity Source Sequence



Step 4. Click on **Submit**.

Defining Authentication Policies and Authorization Profiles

Authentication Policies

Authentication policies define the conditions between the client and ISE node when 802.1X occurs. They define the RADIUS attribute conditions and authentication protocols that are required for successful authentication, as well as for the external or internal database used for validation of machine and user credentials.

The Authentication policy consists of the following elements:

Results: Define authentication protocols

Configure the authentication method between ISE server and client.

In this example, EAP-FAST is defined as the authentication protocol.

Note: We could have chosen to use the default authentication protocol. In this document, we have elected to add the EAP-FAST protocol to provide the reader with experience for creating authentication protocols.

Conditions: Set the RADIUS attributes to match on 802.1X-based RADIUS authentication requests.

ISE ships with pre-defined 802.1X conditions that will be used when configuring policies.

In this example, predefined wireless 802.1X condition rule will be used.

Defining Identity Source Sequence: Authentication policy will use the identity source to validate the end user and machine credentials.

In this example, CorpUsers will be defined as the identity source.

Defining the Authentication Policies

In this document, we will define a Wireless Authentication policy, use EAP-FAST for the authentication protocol, and select CorpUsers as the identity source for credential validation.

Adding EAP-FAST as the Authentication Protocol

The following illustrates adding the EAP-FAST protocol.

Step 1. Select Policy-**>Authentication->Policy Elements->Results->Authentication->Allowed Protocols->Add**.

Step 2. Enter the name of the allowed protocol.

`In this example, EAP-FAST was entered.`

Step 3. Enable **Allow Anonymous In-band PAC provisioning**.

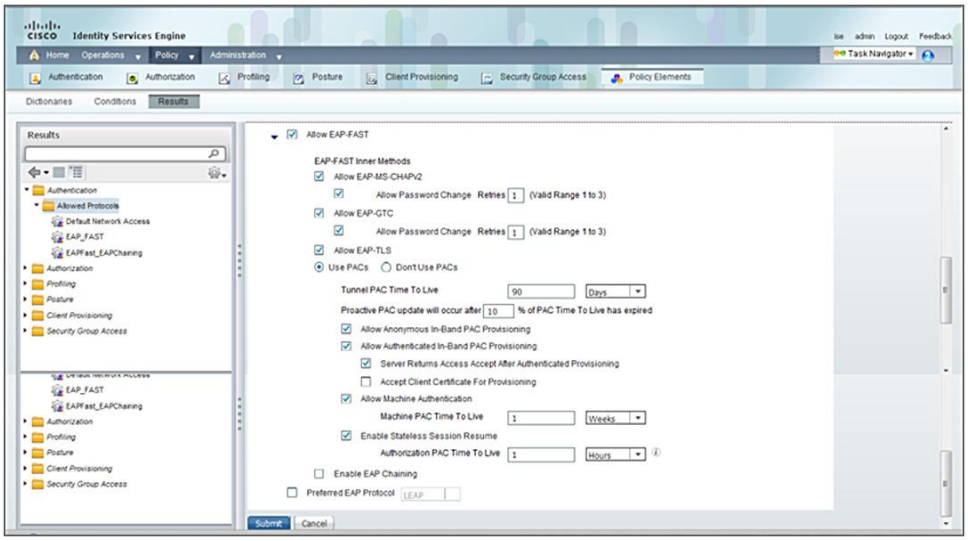
Step 4. Enable **Allow Authenticated In-band PAC provisioning, then enable the following**:

- Server Returns Access Accept After Authenticated Provisioning

Step 5. Enable **Allow Machine Authentication**.

Step 6. Enable **Stateless Session Resume**.

Figure 22. Adding EAP-FAST Authentication Protocol)



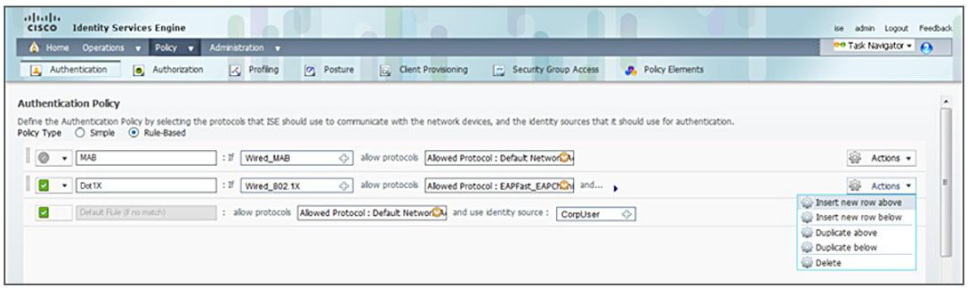
Step 7. Click on **Submit**

Define Authentication Policy

A wireless authentication policy will be created, EAP-FAST selected as the allowed protocol, and CorpUsers selected as the Identity Store.

Step 1. Select **Policy->Authentication->by the gear**, select **Actions**, then insert **new row** above.

Figure 23. Adding Authentication Policy rule



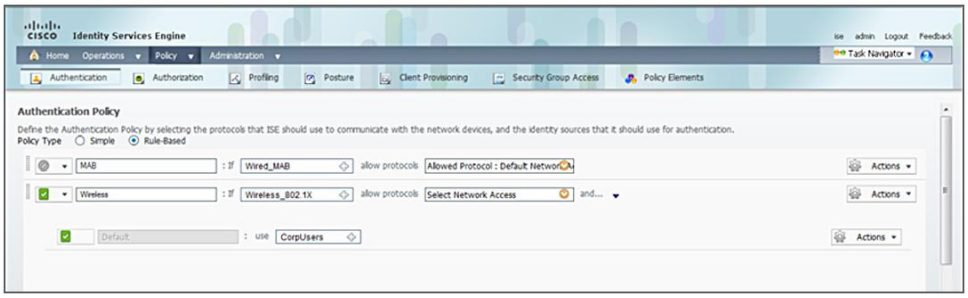
Step 2. Replace standard rule 1 name with wireless.

Step 3. Click on **+** next to Condition(s)

Step 4. Select **Existing Condition** from the library from the drop-down menu, then select ->**Compound Condition->Wireless 802.1X**

Step 5. Click on >, **click** on the **+** next to Internal Users, then select **CorpUsers** for the Identity Source

Figure 24. Authentication Policy



Step 6. Click on **Save**.

Define the Authorization Profiles

Authorization occurs once the end user has successfully authenticated. Authorization policies provide the rules that must be met before the end user is provided with full or restricted network access as determined by the associated authorization profile.

The authorization profile contains common data such as VLAN information and other RADIUS attributes, and consists of the following elements:

Authorization Profile: Defines full or restricted network access.

In this example, we will define one profile to match the authorization condition for wireless, and provide full network access.

Conditions: Contain the authorization rules that determine the required network permissions or level of access

In this example, the default wireless condition rule will be used.

Create Authorization Profile

In this document, we will define, a Wireless Authorization Policy, based on the default wireless 802.1X condition. Then, we will provide the appropriate level of access as defined by the corresponding authorization profile, WIRELESSACCESS

Step 1. Select->**Policy->Authorization->Policy Elements->Results->Authorization->Authorization Profiles->Add**

Step 2. Enter **name of profile**.

`In this example, WIRELESSACCESS was used`

Step 3. Select **VLAN**, and enter **VLAN ID**.

`In this example, VLAN ID 12 was used`

Figure 25. Wireless Authorization Profile

Step 4. Click on Submit.

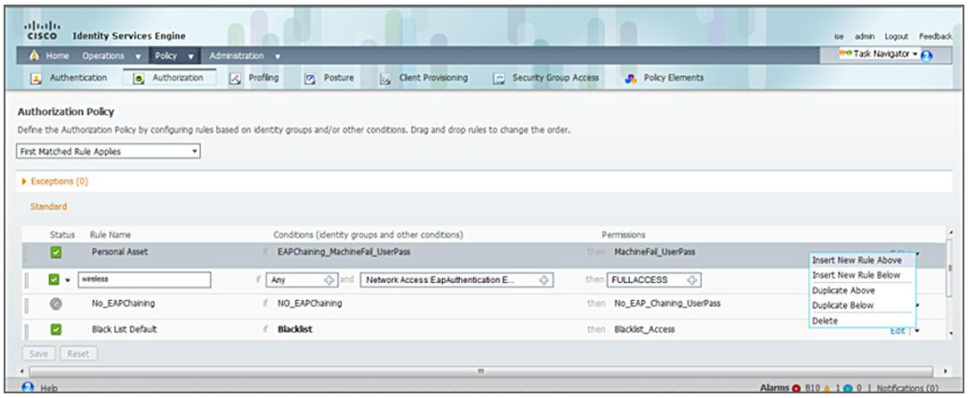
Defining Authorization Condition Rules and Authorization Policies

Once the authorization profile has been created, define the authorization policy rule and the condition rule.

Define Authorization Policy

Step 1. Select->**Policy->Authorization->**, click on the **down arrow**, and Insert **New Rule** above.

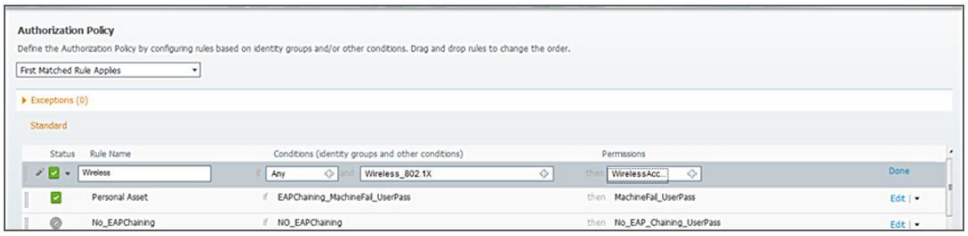
Figure 26. Adding Authorization Policy Rule



Step 2. Replace **standard rule 1 name** with **wireless**, click on + next to **select condition**, and **select wireless 802.1X** for the condition name.

Step 3. Click on the '**+**' sign next to **Authz profile**, then select ->**Standard->Wireless Access**.

Figure 27. Authorization Policy for Wireless



Step 4. Click on **Save**.

Configuring the AnyConnect Network Access Manager

Network Access Manager Installation and Configuration

Installing AnyConnect Network Access Manager

Step 1. Extract the contents of the **AnyConnect ISO image** to a folder

Run **setup**

Note: Please note that you will require local admin rights during the installation.

Step 2. Enable **AnyConnect Diagnostics** and **Reporting Tool**.

Step 3. Enable AnyConnect Network Access Manager

Figure 28. Installation Selector)

Note: You will see the message in Figure 28 after a completed install of the AnyConnect Secure Mobility Client. As part of the core install, the AnyConnect Quality Improvement feature is enabled by default. This feature provides Cisco with customer-installed AnyConnect modules, and enabled features. Crash dumps may also be included. This feature can be completely disabled by using the Profile Editor or just for disabling crash dumps. Corporate privacy is maintained by hashing the machine name; however, crash dumps may contain personal information, which is why the EULA license is displayed.

Figure 29. AnyConnect Quality Improvement Feature

Creating an AnyConnect Network Access Manager Profile with the Profile Editor
The Profile Editor will also be required to configure the AnyConnect Network Access Manager Configuration Profile for EAP-FAST authentication.

Note: Please note that the AnyConnect Network Access Manager configuration should be saved as configuration.xml, and saved to the 'NewConfigFiles' directory. Right-click on the AnyConnect GUI in the system tray, then select 'Network Repair'. This will place the configuration.xml file into the AnyConnect Network Access Manager system directory.

Open the profile editor, and access the current system configuration.

Step 1. Select **file open** from the drop-down menu, and open the **configuration.xml** file as shown in Figure 30.

Figure 30. Opening Configuration.xml file)

Step 2. Keep the defaults, and select**->Networks**.

Step 3. Define your networks.

`In this example, Corporate was defined for the administrative network profile, as illustrated in Fig 31.`

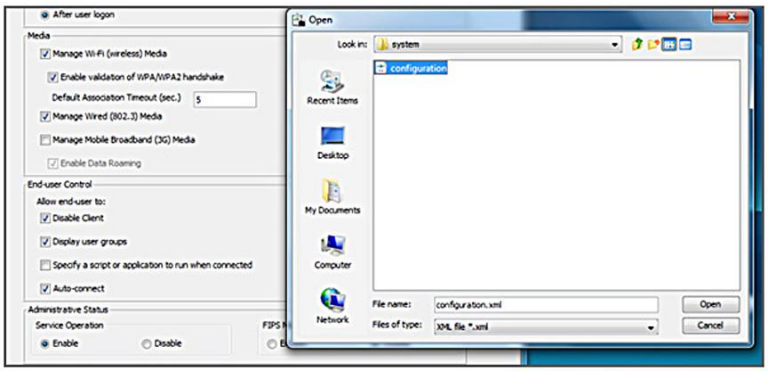
Step 4. Enable **WiFi network, then enter SSID value**.

`In this example, lab005 was used.`

Step 5. Enable the following:

- Hidden Network
- Corporate Network

Figure 31. Wireless Network Profile Description



Step 6. Select ->**Next**.

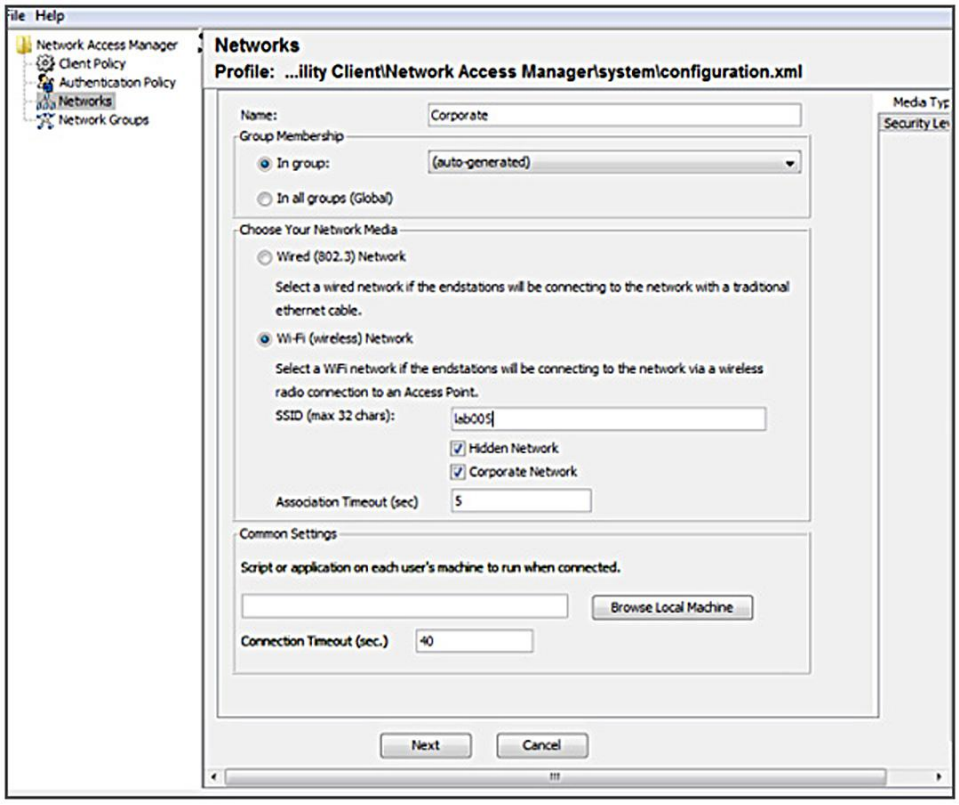
Step 7. Select->**Authenticating Network**.

```
Authenticating Network settings contain the 802.1X settings that contain
MACSec configuration settings, and also 802.1X network connectivity settings
```

Step 8. Under Association Mode, from the drop-down menu, select encryption to match your WLC configuration.

```
In this example, WPA2 enterprise (AES) was selected
```

Figure 32. Network Security Level

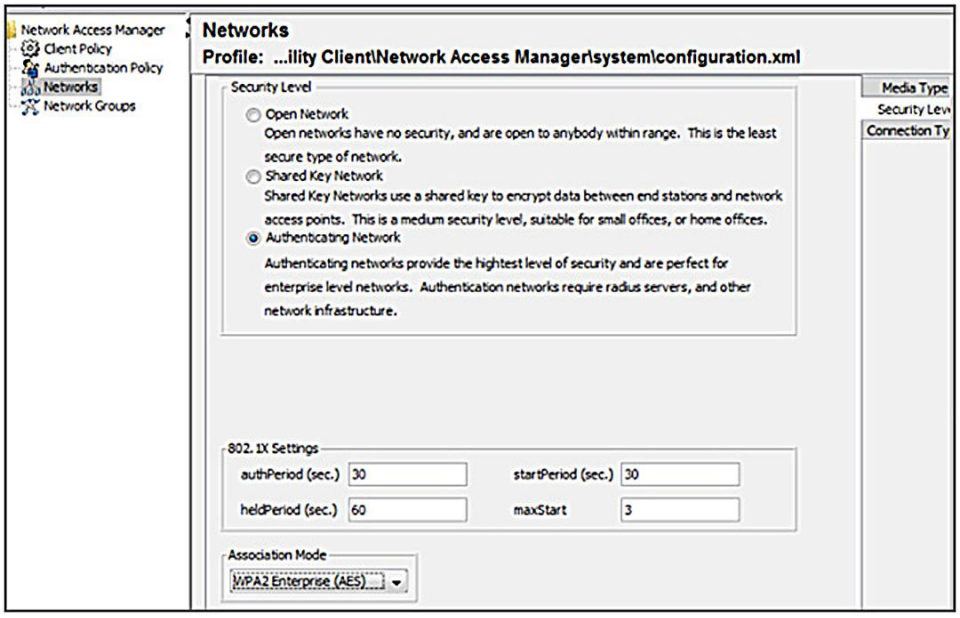


Step 9. Select ->**Next**.

Step 10. Select **Machine and User Connection**.

Note: Machine and User Connection determines the network connection types

Figure 33. Network Connection Type



Step 11. Select->**Next**.

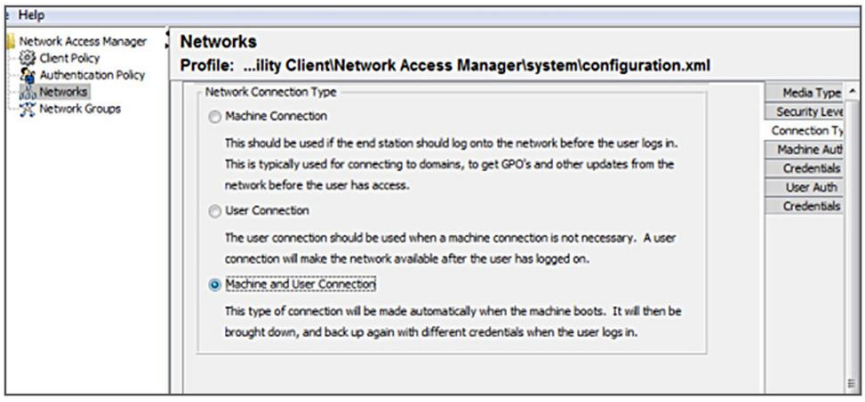
Step 12. Select **EAP-FAST** as the EAP method, then uncheck **Validate Server Identity**.

Note: EAP-FAST will be the method of Authentication, and EAP-MSCHAPv2 will be the inner method.

In this example, root certificate and ISE identity certificate are not installed, which is why Validate Server Identity is unchecked.

Step 13. Leave the defaults.

Figure 34. EAP-FAST Selection

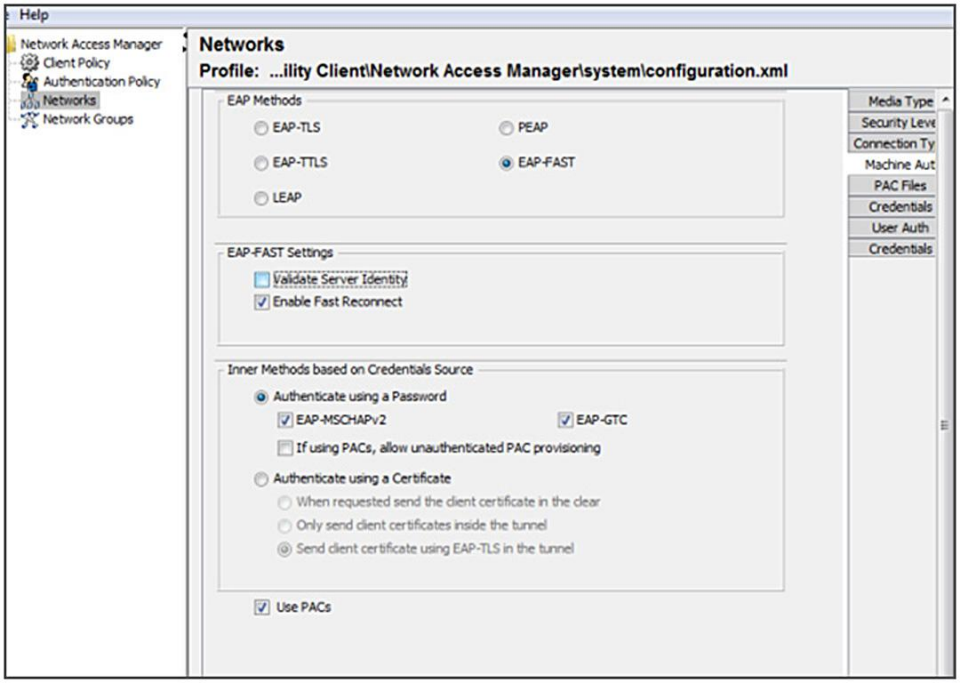


Step 14. Select->**Next**.

Step 15. Leave PAC files set for **empty**, as shown in Figure 22, then select **Next**.

Note: PAC file will be provisioned from ISE

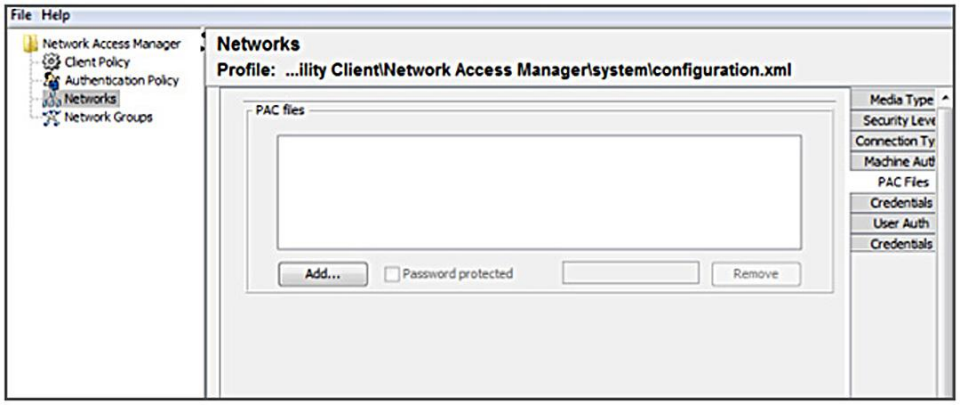
Figure 35. PAC Files



Step 16. Leave defaults for **machine identity**, then select ->**next**.

Note: Machine identity credentials will be sent to the ISE server for validation.

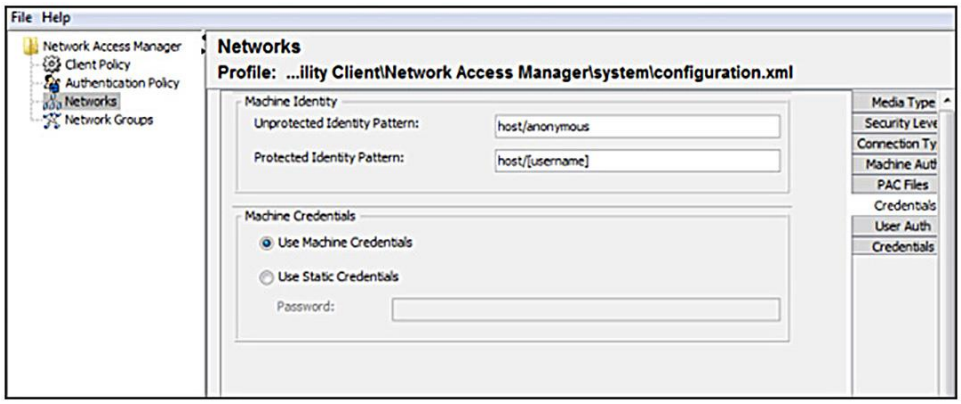
Figure 36. Machine Identity Credentials



Step 17. Select ->**EAP-FAST** for user authentication, then uncheck **Validate Server Identity**.

Step 18. Leave the defaults.

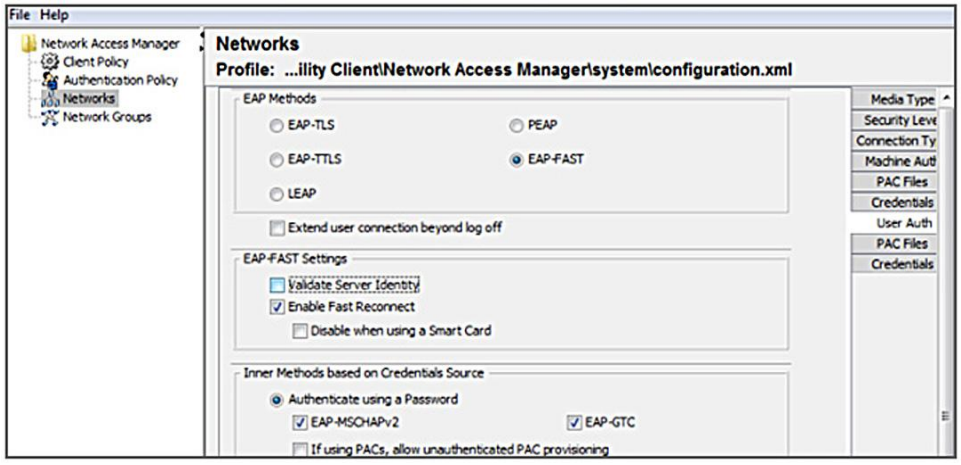
Figure 37. EAP-FAST for user authentication



Step 19. Select -> **Next**.

Step 20. Leave PAC files empty, then select ->**Next**.

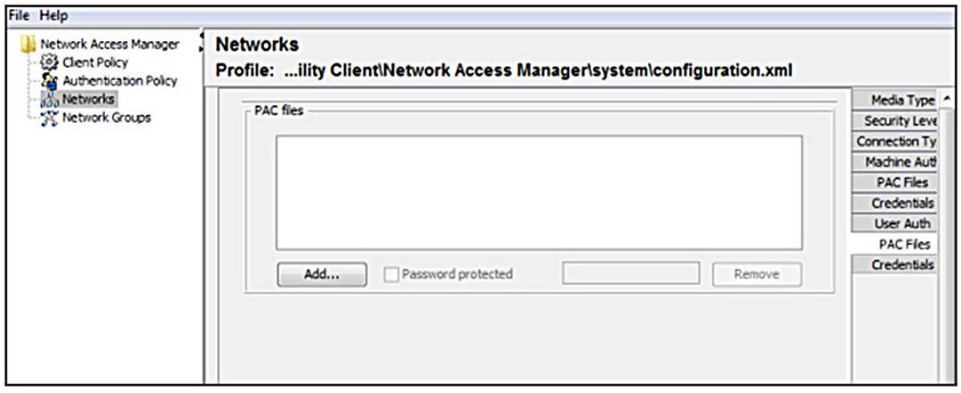
Figure 38. PAC Files



Step 21. Leave the defaults for user credentials.

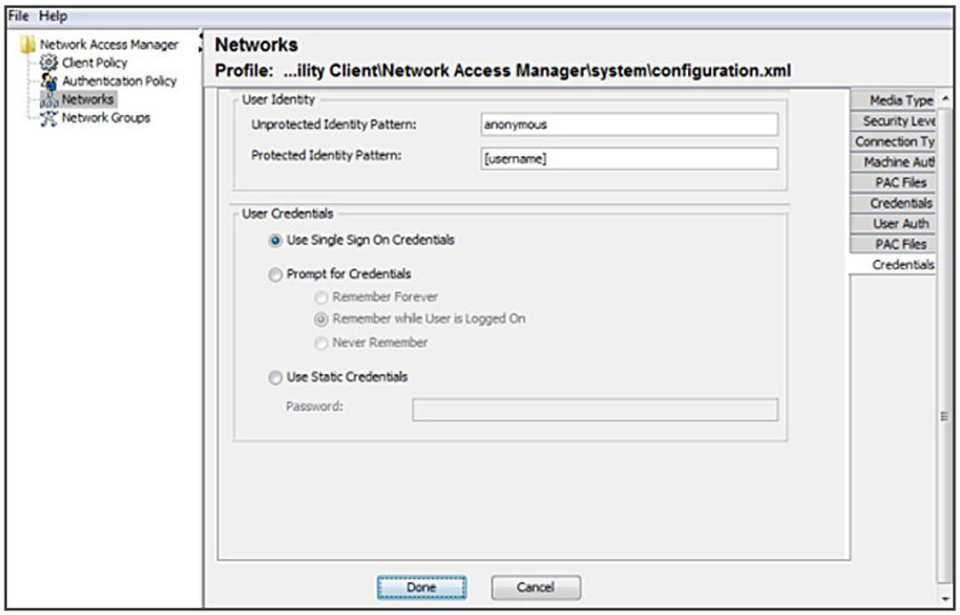
Note: User credentials will be sent to the ISE server for validation

Figure 39. User Identity Credentials



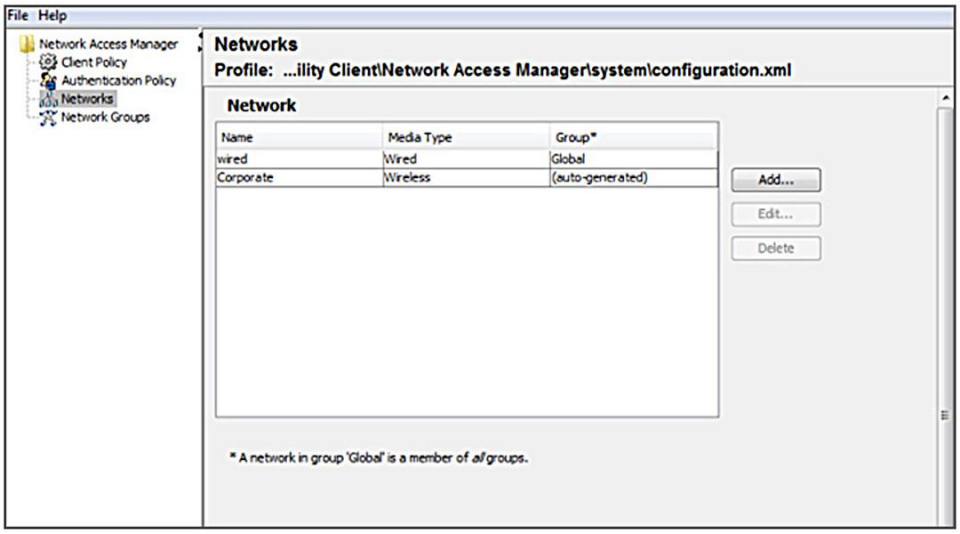
Step 22. Select->**Done**.

Figure 40. Completed Profile



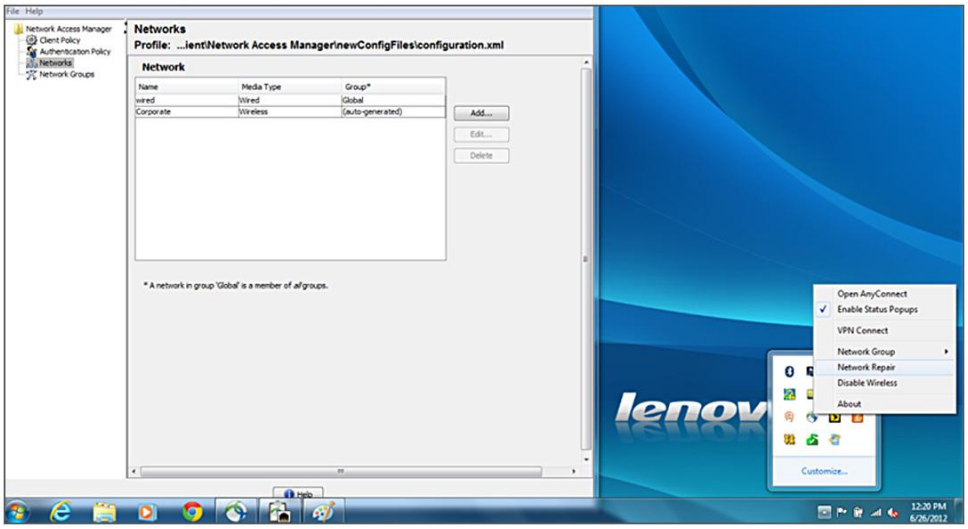
Step 23. Click **file** and save as **configuration.xml**.

Figure 41. Saving configuration.xml



Step 24. Run **network repair**, then right-click on **AC GUI**, and click on **Network Repair**.

Figure 42. Run Network Repair



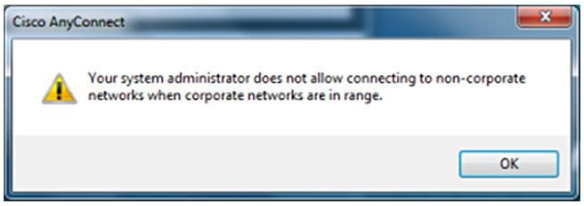
Testing Procedure

- Click on the **AC GUI**, and then connect to **Corporate**.

Figure 43. Connect to Corporate

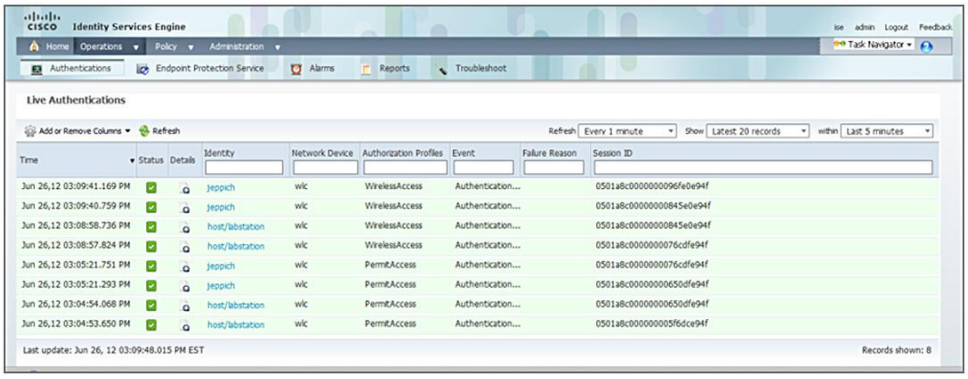
- Click on any other **non-corporate APs**. You should see the following error message:

Figure 44. Non-Corporate Connection



- View the **ISE Authentication Live Logs**. You will see separate transactions for successful machine and user credentials.

Figure 45. Live Authentication Logs



Appendices

Configuring the Switch for Multiple VLANs

In order to allow multiple VLANs through the switch, the following commands were configured on the switch port connecting to the controller:

interface GigabitEthernet1/0/6

description Trunk Port to WLC

switchport trunk encapsulation dot1q

switchport mode trunk

Interface VLAN Configuration is listed below:

Interface VLAN12

Description of AP VLAN

ip address 10.3.1.2 255.255.255.0

Gigabit Switch Port Configuration is listed below:

Interface Gigabit Ethernet 1/0/10

Description of access port connection to Cisco AP

switchport access vlan 12

switchport mode access

Configure the WLC for Basic Operation and Register the Lightweight APs to the Controller

Use the startup configuration wizard on the command-line interface (CLI) to configure the WLC for basic operation. Alternatively, you can also use the GUI to configure the CLI. This document explains the configuration on the WLC with the startup configuration wizard on the CLI.

After the WLC boots the first time, it enters into the startup configuration wizard. Use the configuration wizard to configure basic settings. You can access the wizard using the CLI or the GUI. The output shows an example of the startup configuration on the GUI:

Welcome to the Cisco Wizard Configuration Tool

Use the '-' character to backup

System Name: Cisco_63:75:80

Enter Administrative User Name (24 characters max): jeppich

Enter Administrative Password (24 characters max): *******

Management Interface IP Address: 192.168.1.5

Management Interface Netmask: 255.255.255.0

Management Interface Default Router: 192.168.1.1

Management Interface VLAN Identifier (0=tagged):

Management Interface DHCP Server IP Address: 192.168.1.1

AP Manager Interface IP Address: 192.168.1.6

AP Manager is on Management subnet, using same values

AP Manager Interface DHCP Server 192.168.1.1

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: lab005

Network Name (SSID): lab005

Allow Static IP Addresses [YES][no] yes

Configure a Radius Server now [YES][no] yes

Enter Country Code (enter 'help' for a list of countries) (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

Configuration saved!

Resetting system with new configuration

These parameters set up the WLC for basic operation. In this example configuration the WLC uses 192.168.1.5 as the management interface IP address and 192.168.1.6 as the AP-manager interface IP address.

Before any other features can be configured on the WLC, the Lightweight APs have to register with the WLC. This document assumes that the Lightweight AP is registered to the WLC.

Refer to the “Register the Lightweight AP to the WLC section of WLAN Controller Failover for Lightweight Access Points Configuration Example” for information on how the Lightweight APs register with the WLC. For reference with this configuration example, the AP 1130 is deployed on the same subnet.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C07-713768-00 08/12