Configure 802.1x Authentication with PEAP, ISE 2.1 and WLC 8.3

Contents

Introduction

This documents describes how to set up a Wireless Local Area Network (WLAN) with 802.1x security and Virtual Local Area Network (VLAN) override with Protected Extensible Authentication Protocol (PEAP) as Extensible Authentication Protocol (EAP).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 802.1x
- PEAP
- Certification Authority (CA)
- Certificates

Components Used

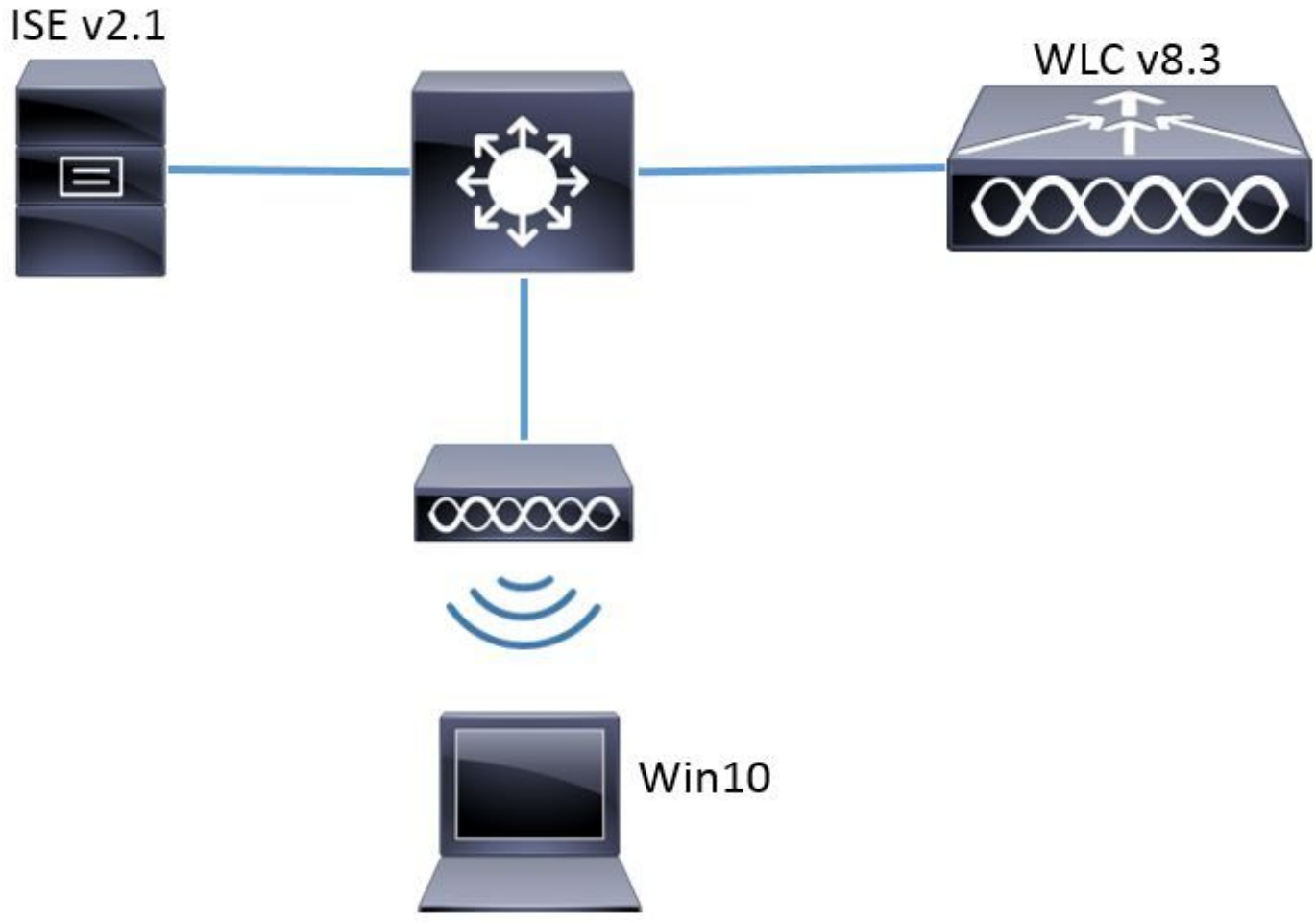
The information in this document is based on these software and hardware versions:

- WLC v8.3.102.0
- Identity Service Engine (ISE) v2.1
- Windows 10 Laptop

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.

Configure

Network Diagram



Configuration

The general steps are:

1. Declare RADIUS Server on WLC and vice versa to allow communication with each other.
2. Create the Service Set Identifier (SSID) in the WLC.
3. Create the authentication rule on ISE.
4. Create the authorization profile on ISE.

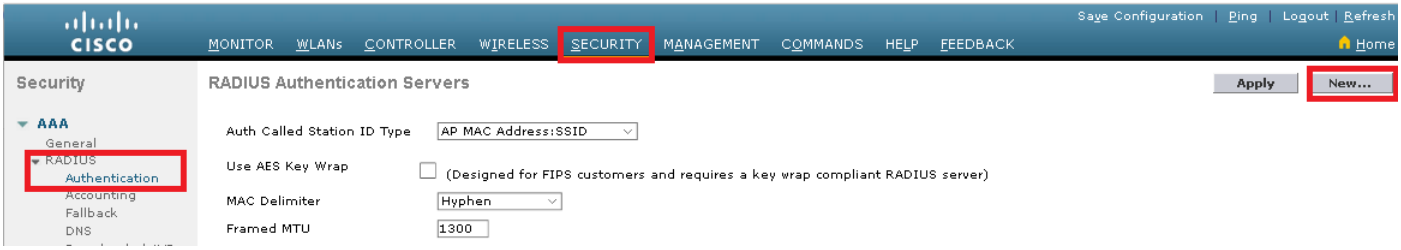
5. Create the authorization rule on ISE.
6. Configure the endpoint.

Declare RADIUS Server on WLC

In order to allow communication between RADIUS server and WLC, it is needed to register RADIUS server on WLC and vice versa.

GUI:

Step 1. Open the GUI of the WLC and navigate to **SECURITY > RADIUS > Authentication > New** as shown in the image.



Step 2. Enter the RADIUS server information as shown in the image.

CLI:

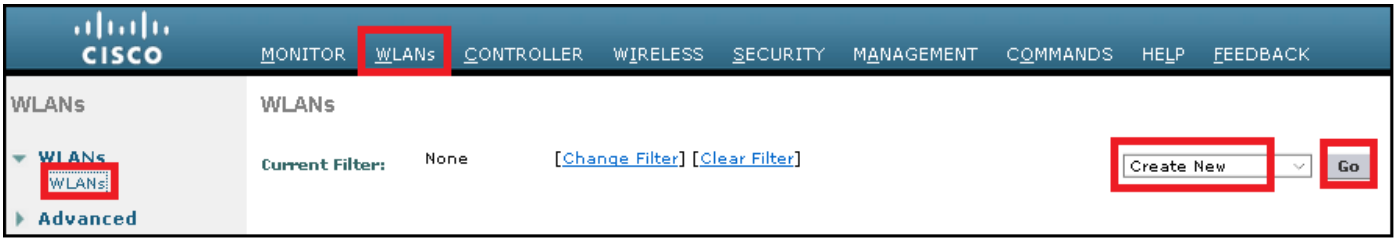
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

<a.b.c.d> corresponds to the RADIUS server.

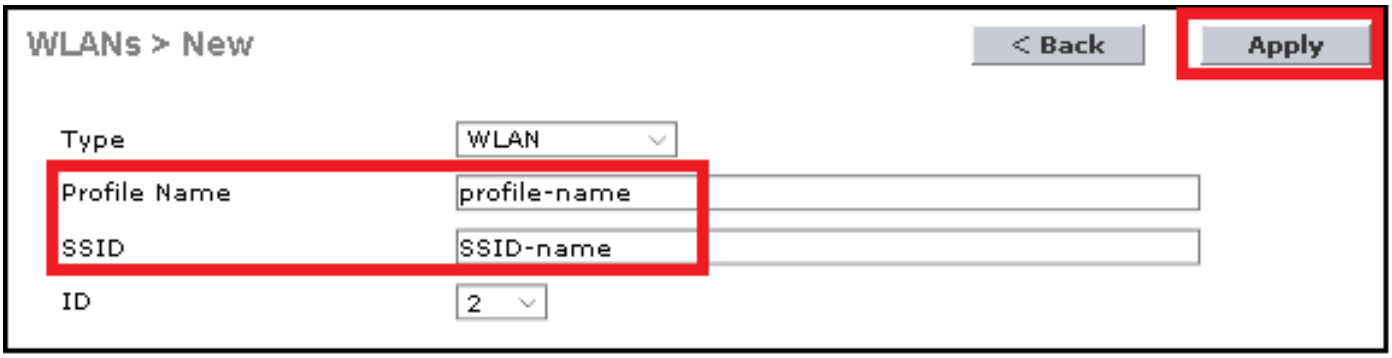
Create SSID

GUI:

Step 1. Open the GUI of the WLC and navigate to **WLANs > Create New > Go** as shown in the image.



Step 2. Choose a name for the SSID and profile, then click **Apply** as shown in the image.



CLI:

```
> config wlan create <id> <profile-name> <ssid-name>
```

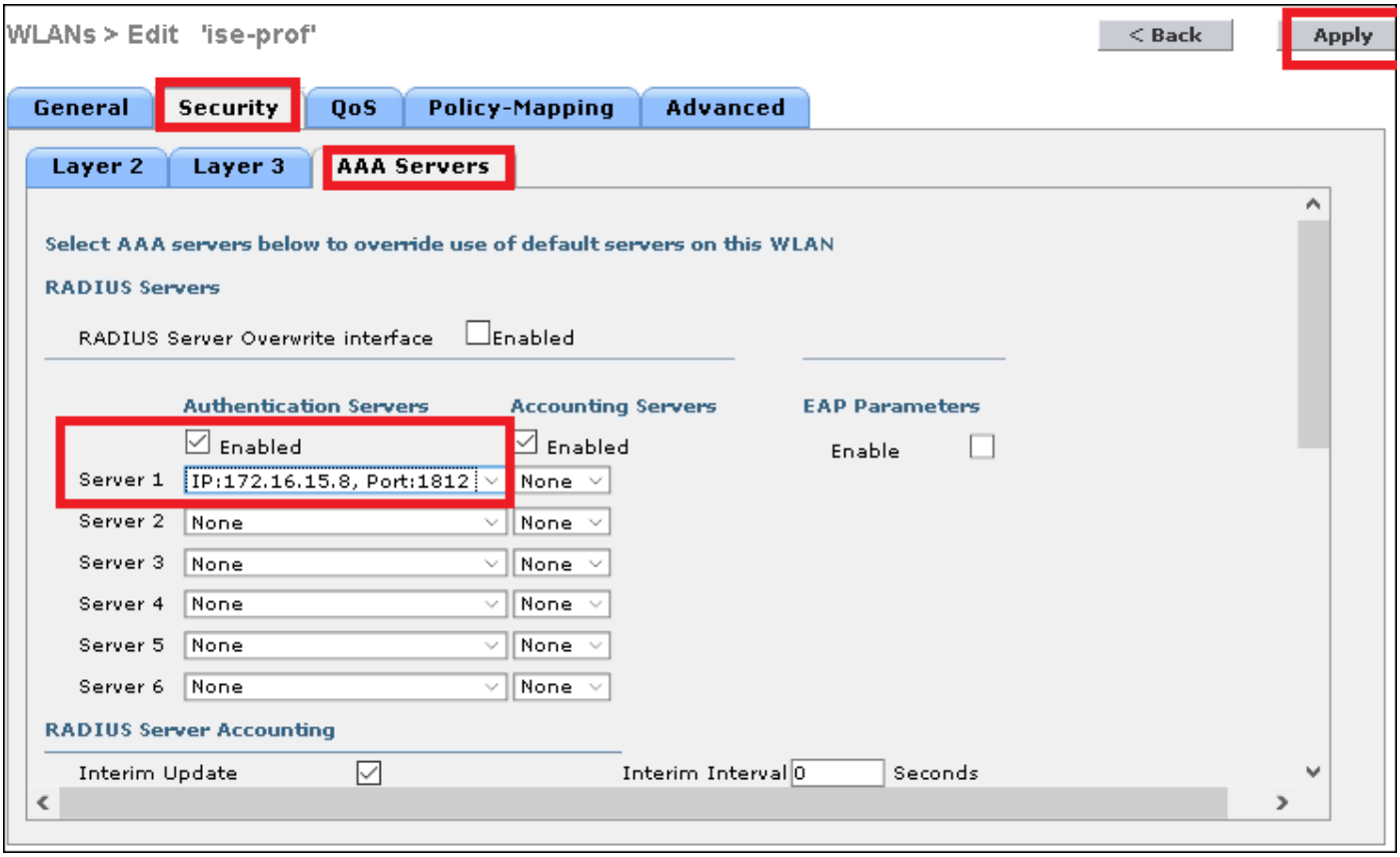
Step 3. Assign the RADIUS server to the WLAN.

CLI:

```
> config wlan radius_server auth add <wlan-id> <radius-index>
```

GUI:

Navigate to **Security > AAA Servers** and choose the desired RADIUS server, then hit **Apply** as shown in the image.



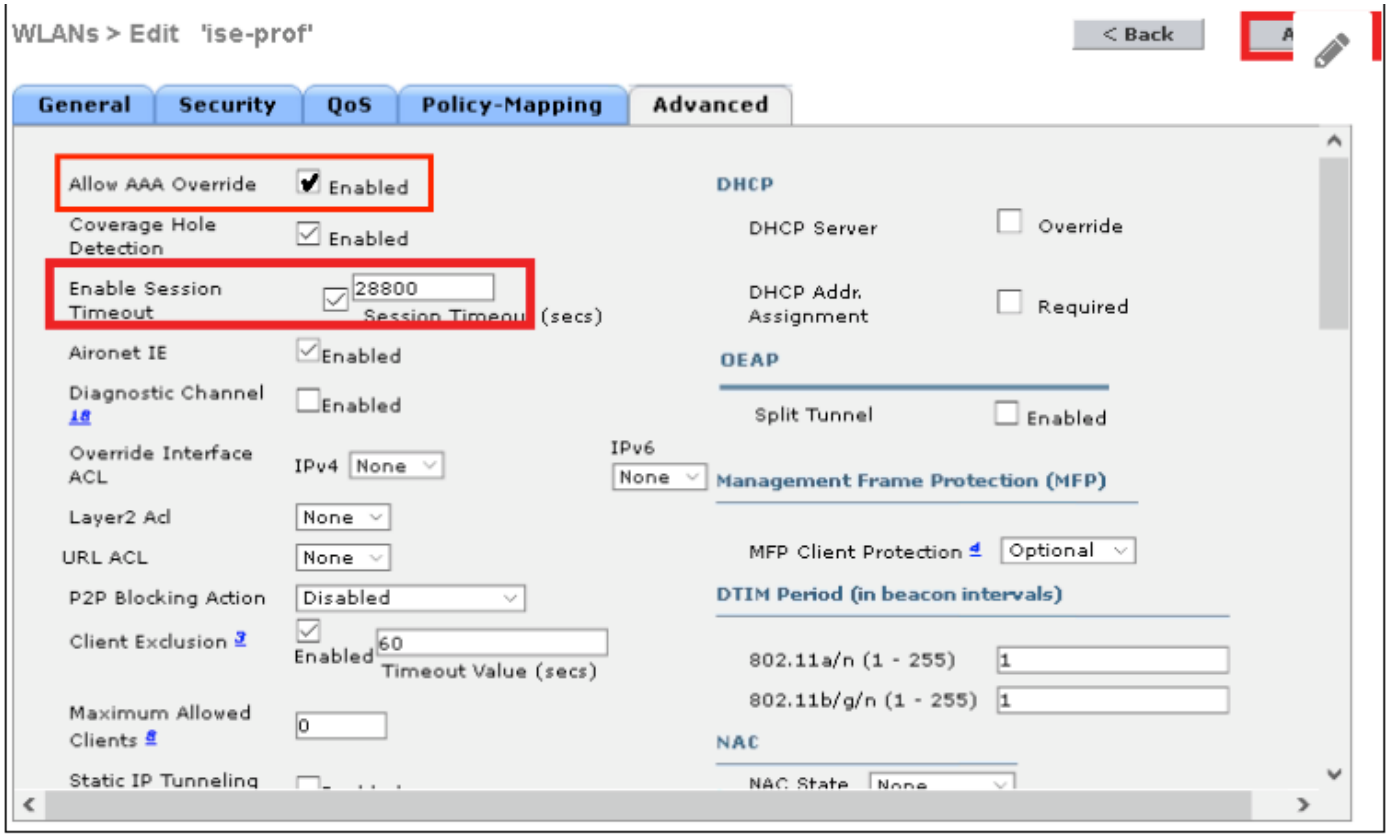
Step 4. Enable **Allow AAA Override** and optionally increase the session timeout

CLI:

```
> config wlan aaa-override enable <wlan-id>
>config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI:

Navigate to **WLANs > WLAN ID > Advanced** and enable **Allow AAA Override**, optionally specify the Session Timeout as shown in the image.



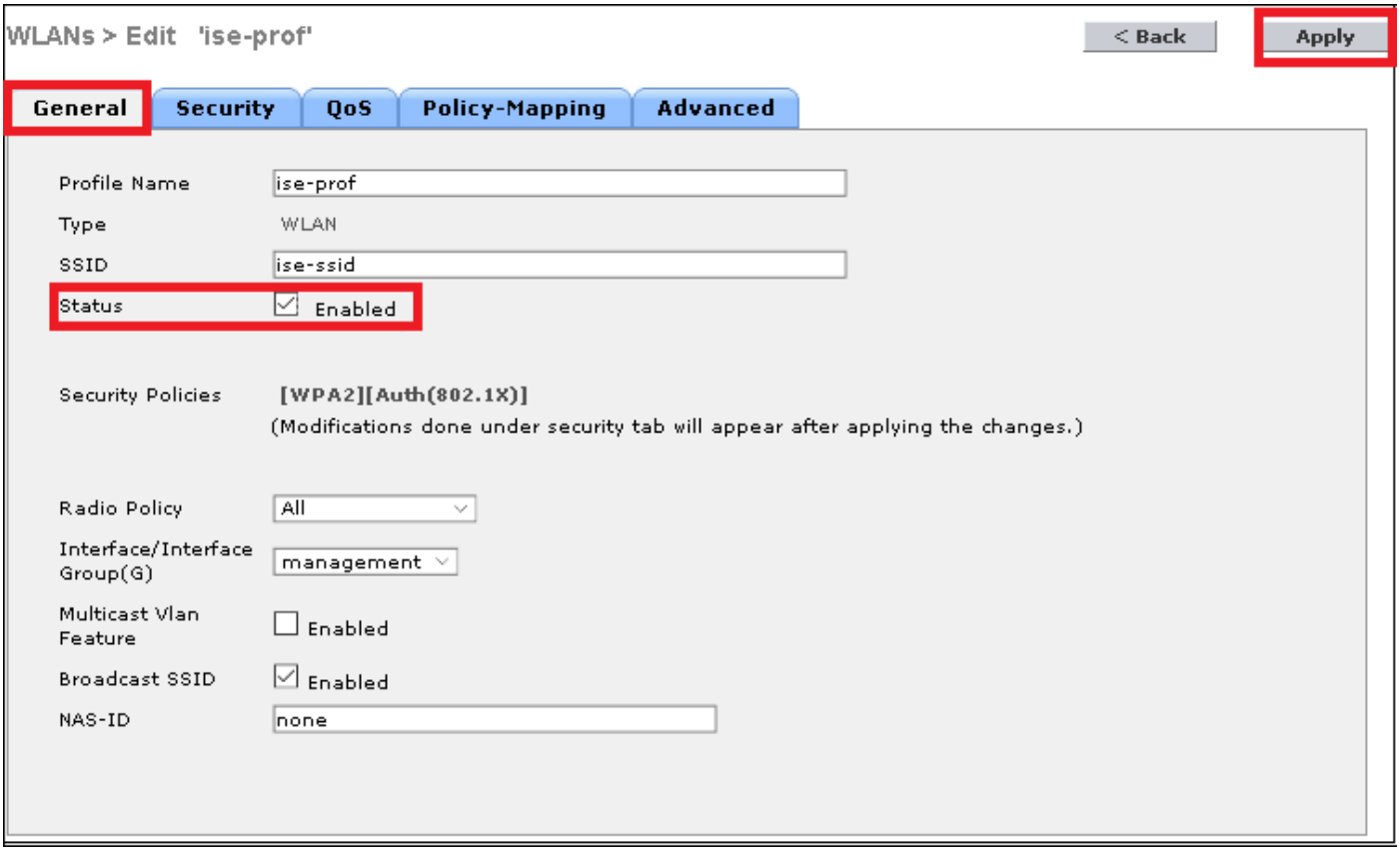
Step 5. Enable the WLAN.

CLI:

```
> config wlan enable <wlan-id>
```

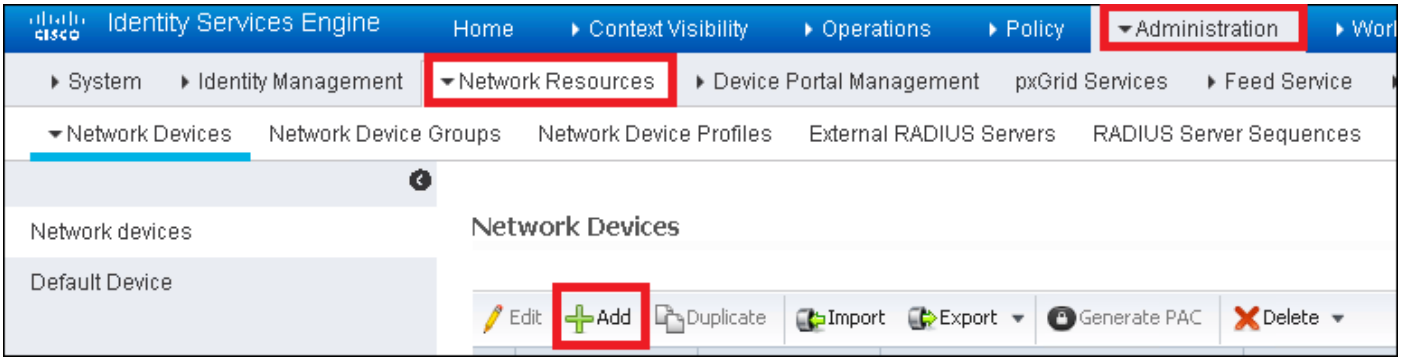
GUI:

Navigate to **WLANs > WLAN ID > General** and enable the SSID as shown in the image.



Declare WLC on ISE

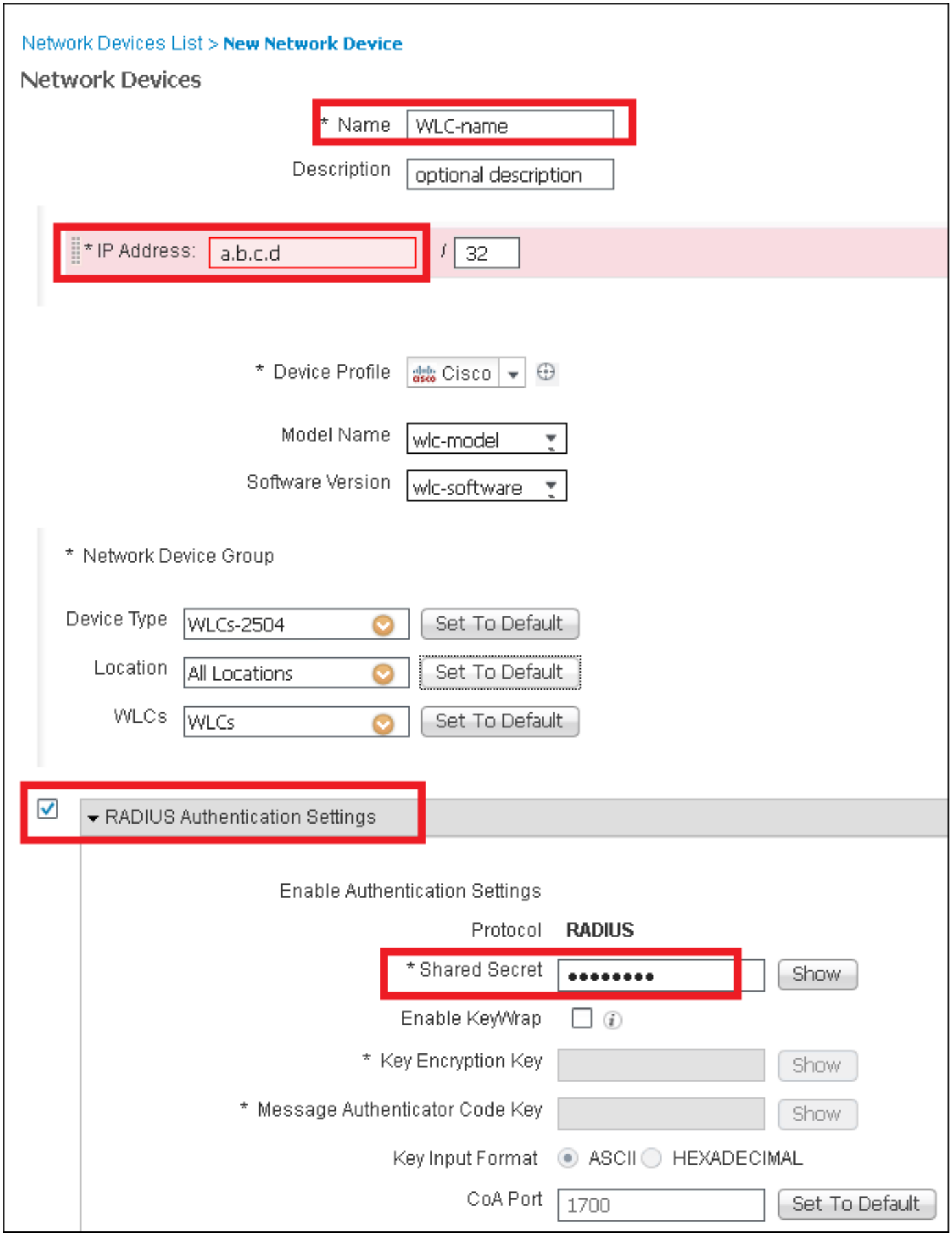
Step 1. Open ISE console and navigate to **Administration > Network Resources > Network Devices > Add** as shown in the image.



Step 2. Enter the values.

Optionally, it can be a specified Model name, software version, description and assign Network Device groups based on device types, location or WLCs.

a.b.c.d correspond to the WLC's interface that sends the authentication requested. By default it is the management interface as shown in the image.

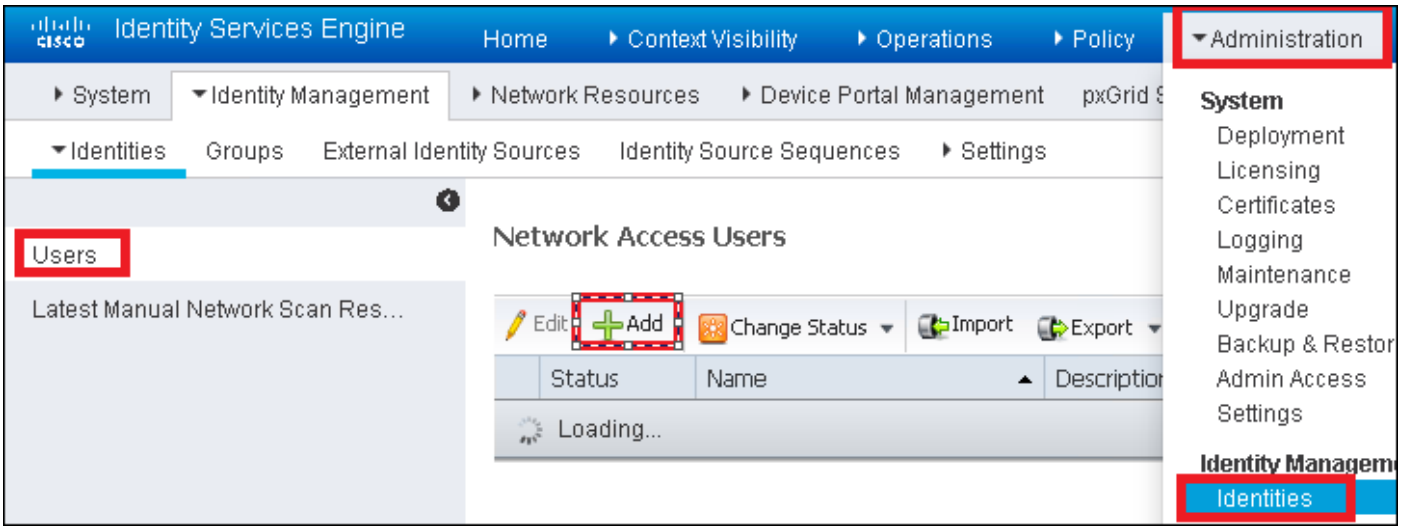


For more information about **Network Device Groups** review this link:

[ISE - Network Device Groups]

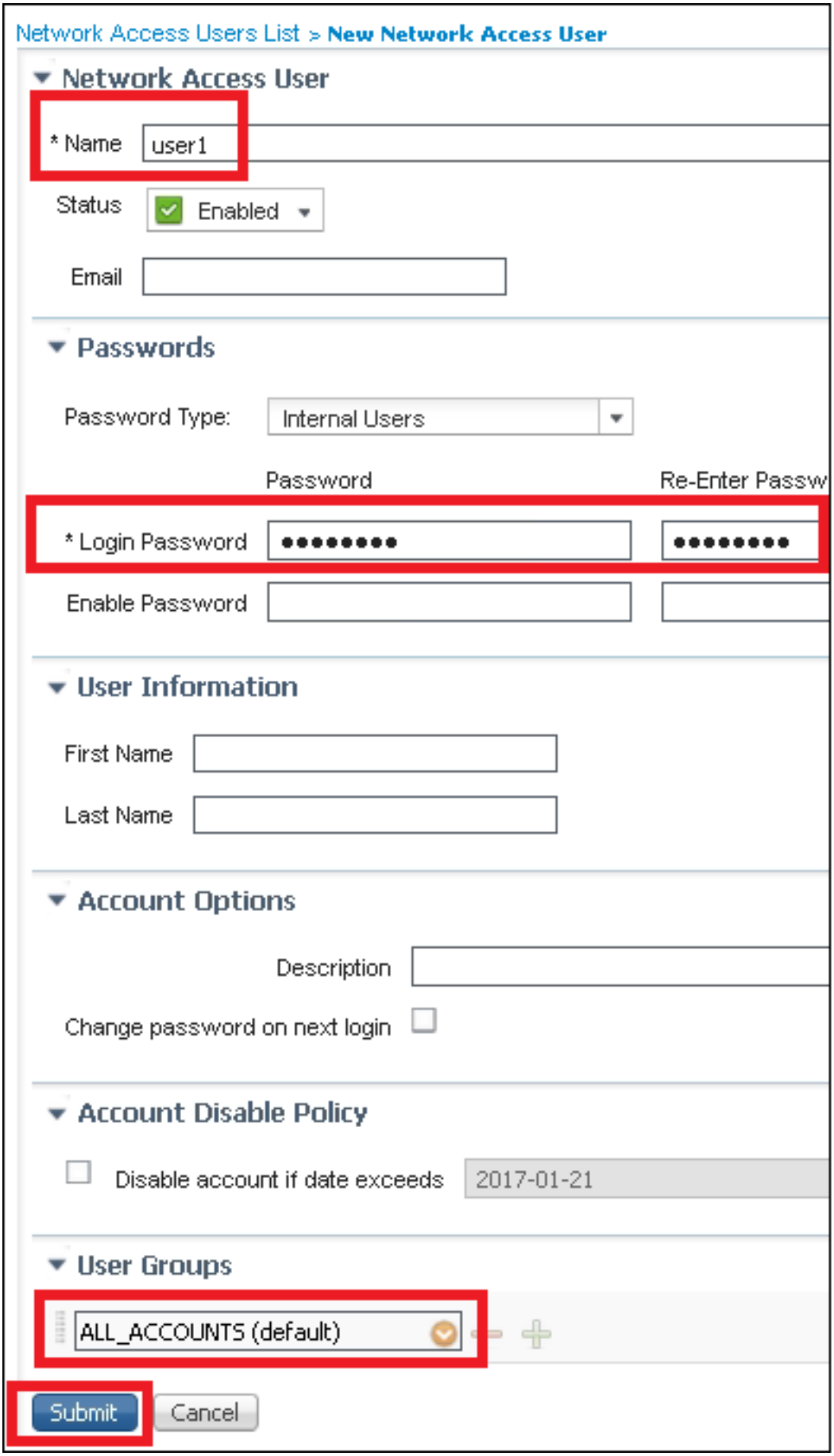
Create New User on ISE

Step 1. Navigate to **Administration > Identity Management > Identities > Users > Add** as shown in the image.



Step 2. Enter the information.

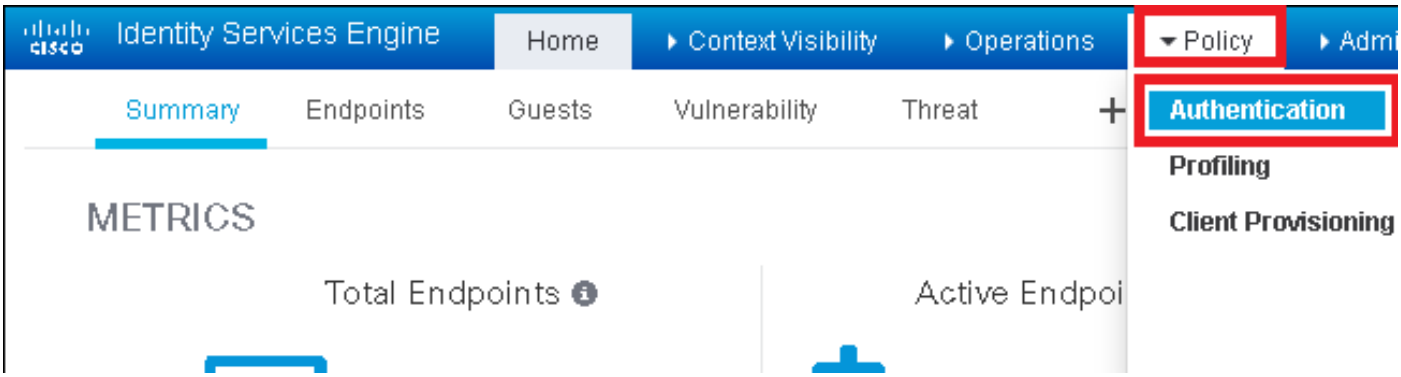
In this example, this user belongs to a group called ALL_ACCOUNTS but it can be adjusted as needed as shown in the image.



Create Authentication Rule

Authentication rules are used to verify if the credentials of the users are right (verify if the user really is who it says it is) and limit the authentication methods that are allowed to be used by it.

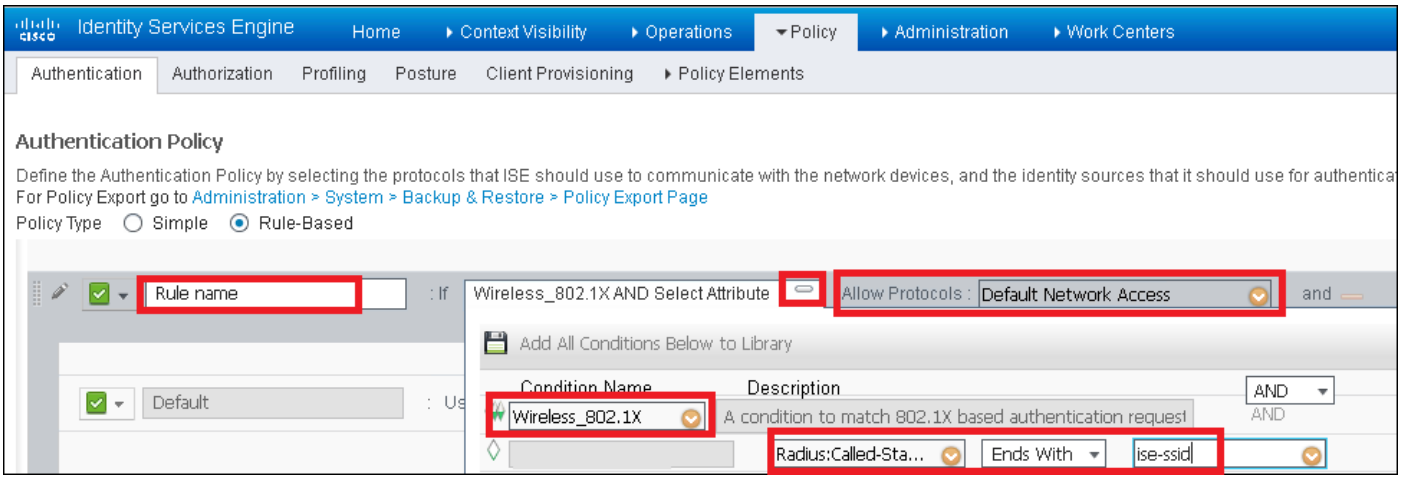
Step 1. Navigate to **Policy > Authentication** as shown in the image.



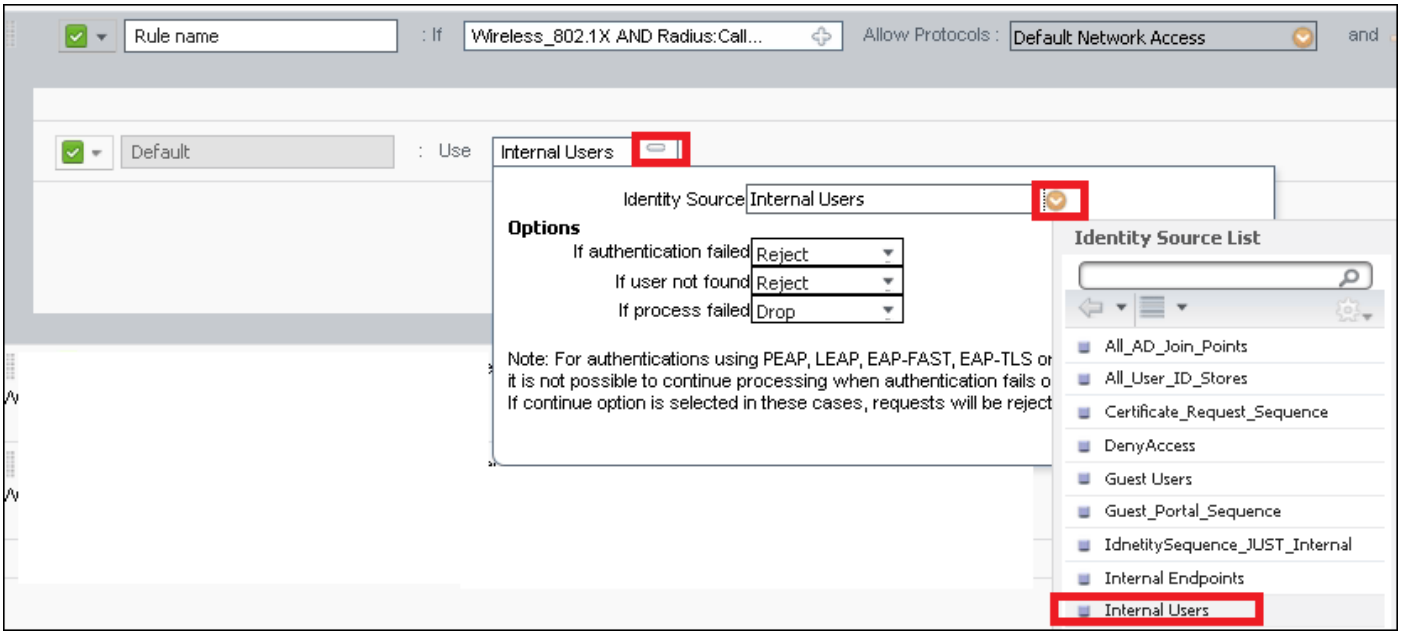
Step 2. Insert a new authentication rule as shown in the image.

Step 3. Enter the values.

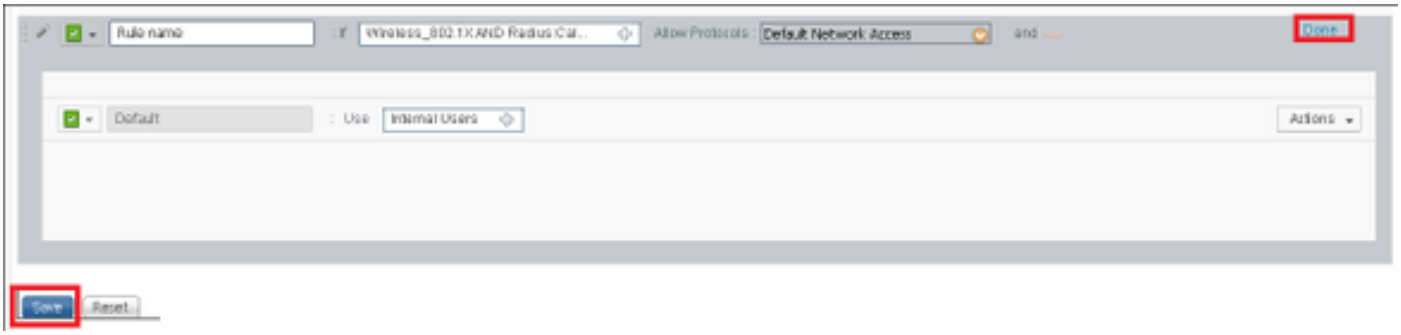
This authentication rule allows all the protocols listed under the **Default Network Access** list, this applies to the authentication request for Wireless 802.1x clients and with Called-Station-ID and ends with **ise-ssid** as shown in the image.



Also, choose the Identity source for the clients that matches this authentication rule. This example uses **Internal users** identity source list as shown in the image.



Once finished, click **Done** and **Save** as shown in the image.



For more information about Allow Protocols Policies consult this link:

[Allowed Protocols Service]

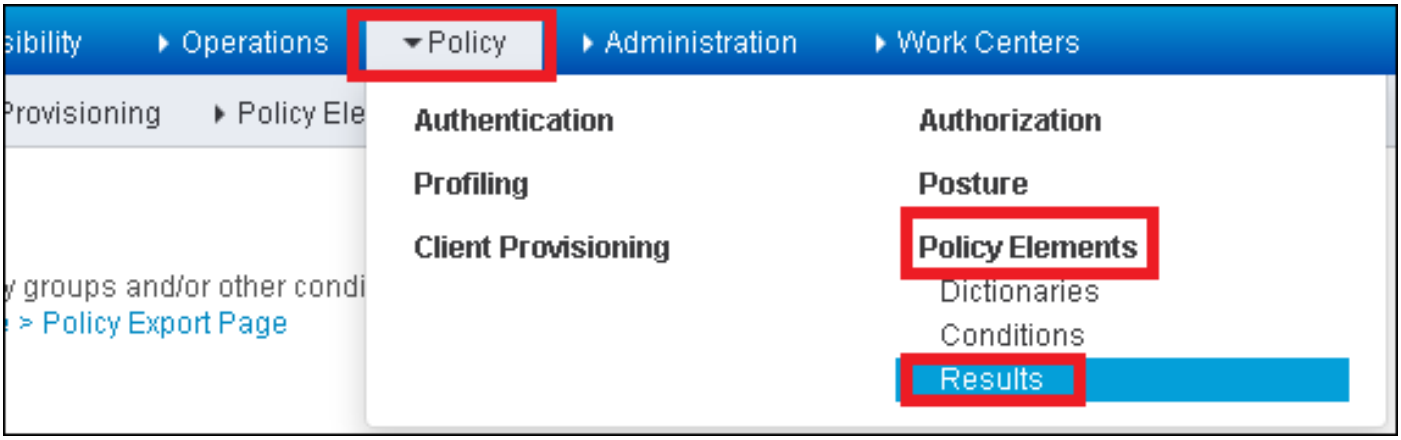
For more information about Identity sources consult this link:

[Create a User Identity Group]

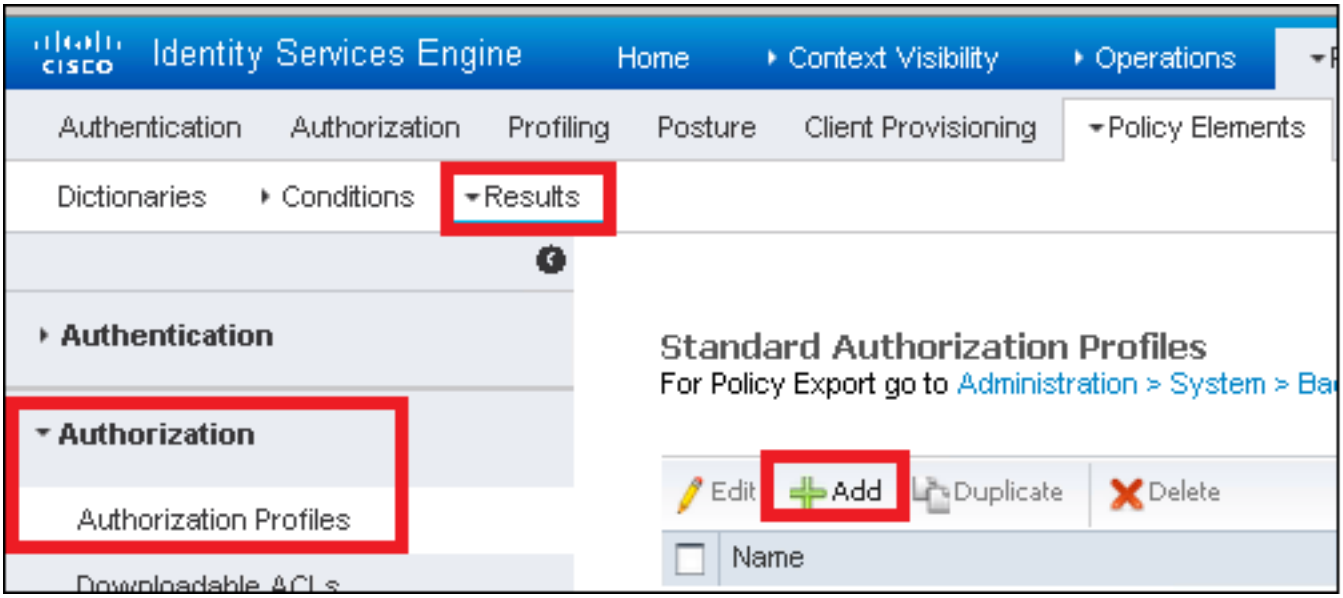
Create Authorization Profile

The authorization profile determines if the client has access or not to the network, push Access Control Lists (ACLs), VLAN override or any other parameter. The authorization profile shown in this example sends an access accept for the client and assigns the client to VLAN 2404.

Step 1. Navigate to **Policy > Policy Elements > Results** as shown in the image.



Step 2. Add a new Authorization Profile. Navigate to **Authorization > Authorization Profiles > Add** as shown in the image.



Step 3. Enter the values as shown in the image.