Policy Enforcement on Mist with Cisco ISE

Role-Based Policy Enforcement

Use Radius Attributes in order to enforce policy using WxLAN

Example Use-case:
Same SSID to be used for Employees and Contractors in an Enterprise Network
Policy enforcement required:

- ➔ Employees need access to All Network Resources
- ➔ Contractors need access to All Network Resources except internal servers

There are two steps required to achieve the above:

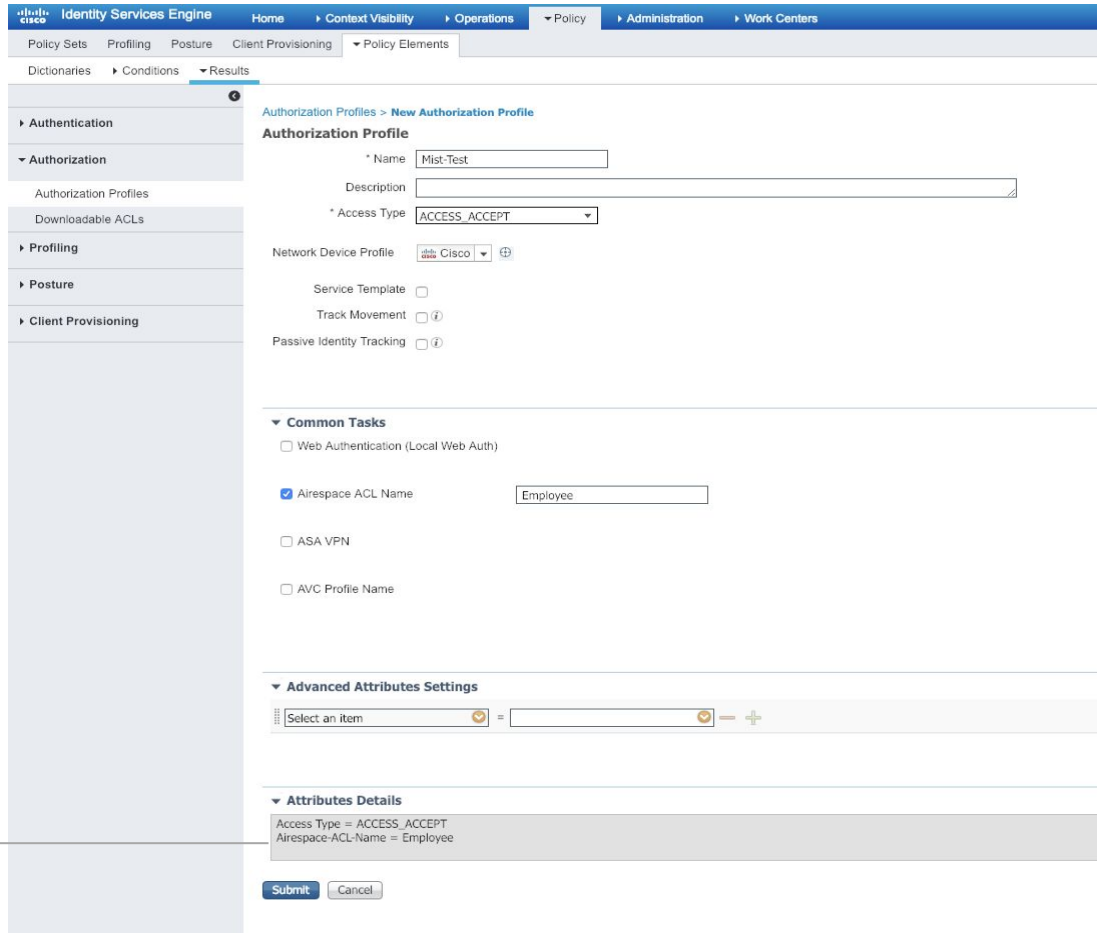
- ❑ Role Indentification:
  - ❑ When a user attempts to authenticate, the Radius server verifies the credentials with AD (or any external/internal sources), based on the attribute, returns the ACCESS_ACCEPT with appropriate AVP(Attribute-Value-Pairs). These AVPs are used by Mist to identify and tag a resource appropirately.
- ❑ Policy Enforcement:
  - ❑ Based on the WxLAN is used to enforce the above policy

Role-Based Policy Enforcement

ISE Configuration

1) Create the Authorization profile including the AVP pair to be sent to Authenticator

Policy -> Result-> Authorization -> Authorization Profiles -> Add



In this AVP
A = Airespace-ACL-Name
V = Employee

Role-Based Policy Enforcement

ISE Configuration

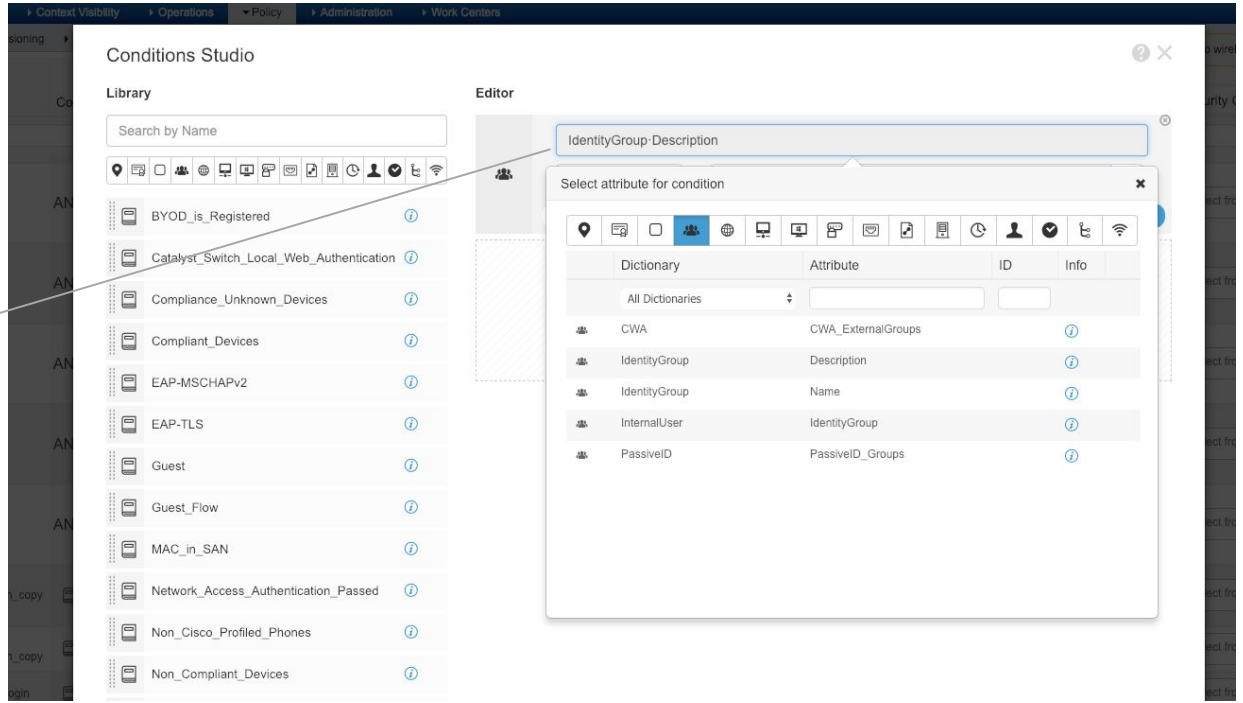
2) As an example, to identify the user, we are using Identity Group

a) Policy -> Policy Sets-> Default Policy-> Authorization Policy -> Insert Rule Above Basic Authenticated Access

b) Name the policy
- Employee_Policy

c) Click on + in Conditions

Choose Identity Group and provide corresponding value and name it as Employee



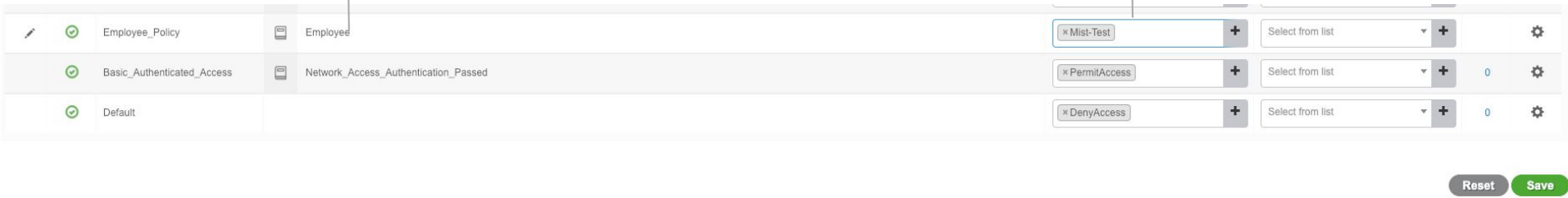
Role-Based Policy Enforcement

ISE Configuration

3) Associate the group (Created in Step 2) to the corresponding Authorization Policy we created in Step 1

The AD Group to which the client belongs to

The corresponding Policy that includes required AVP



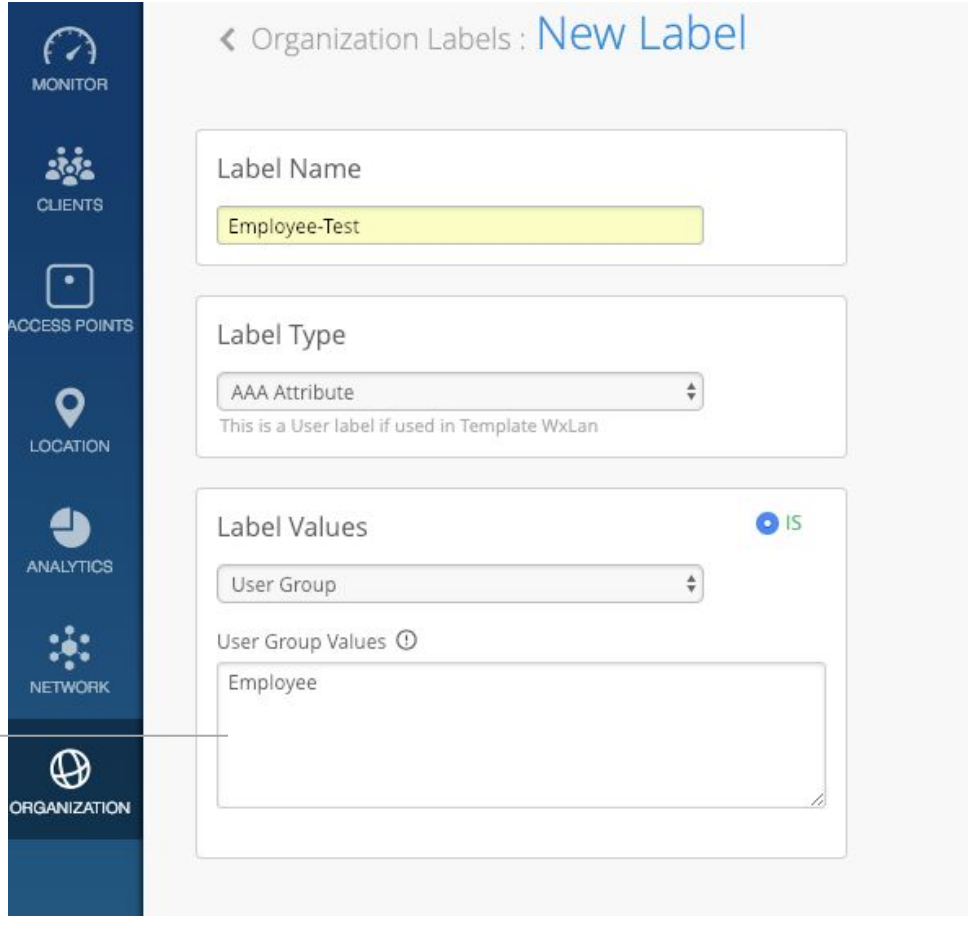
Role-Based Policy Enforcement

Mist Configuration
Need to tie the AVP from ISE to WxLAN

1) Configure the Label
   a) Create a label*
   b) Choose Lable Type: AAA Attribute
   c) Choose Label Values: User Group

*Note: Both Org and Site Labels are supported for this feature

The string should be an exact match to the value in the AVP we created in Step 1 on ISE Config



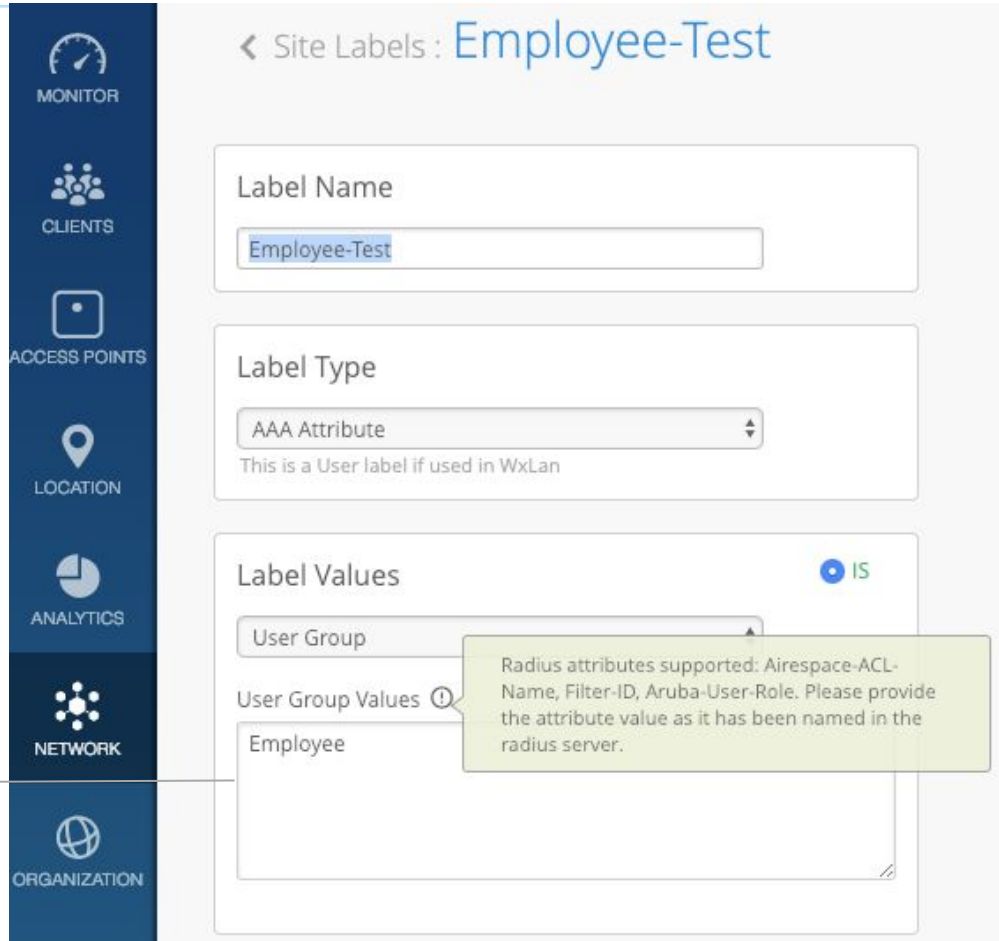
Role-Based Policy Enforcement

Mist Configuration

1) Create the Label
   a) Need to tie the AVP from ISE to WxLAN
   b) Choose Lable Type: AAA Attribute
   c) Choose Label Values: User Group

Note: Label Could be at Org or Site Level

The string should be an exact match to the value in the AVP we created in Step 1 on ISE Config



Role-Based Policy Enforcement

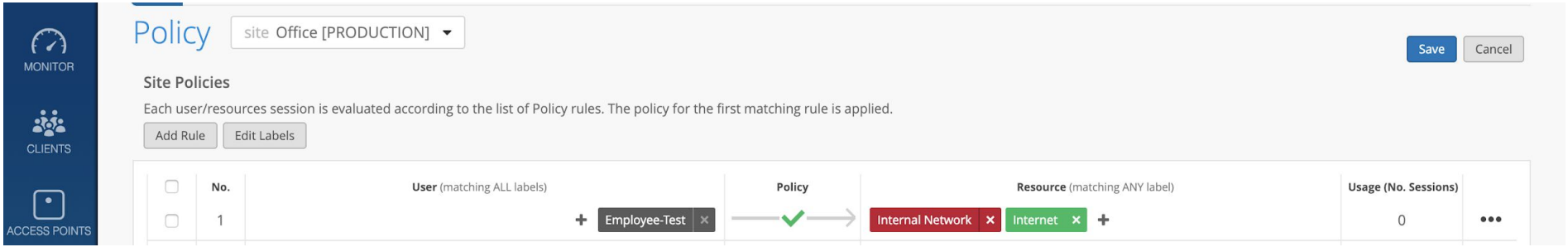
Mist Configuration

2) Create the Policy

a) Use the User tag on the left-hand side as the source (configured in step 1) for the policy

b) Choose the destination and also choose the policy (allow or deny).

c) In the example below, employees not allowed on Internet but are allowed to the internet.



Thankyou