

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 Identification:
 - ❑ 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 appropriately.
- ❑ Policy Enforcement:
 - ❑ Based on the WxLAN is used to enforce the above policy

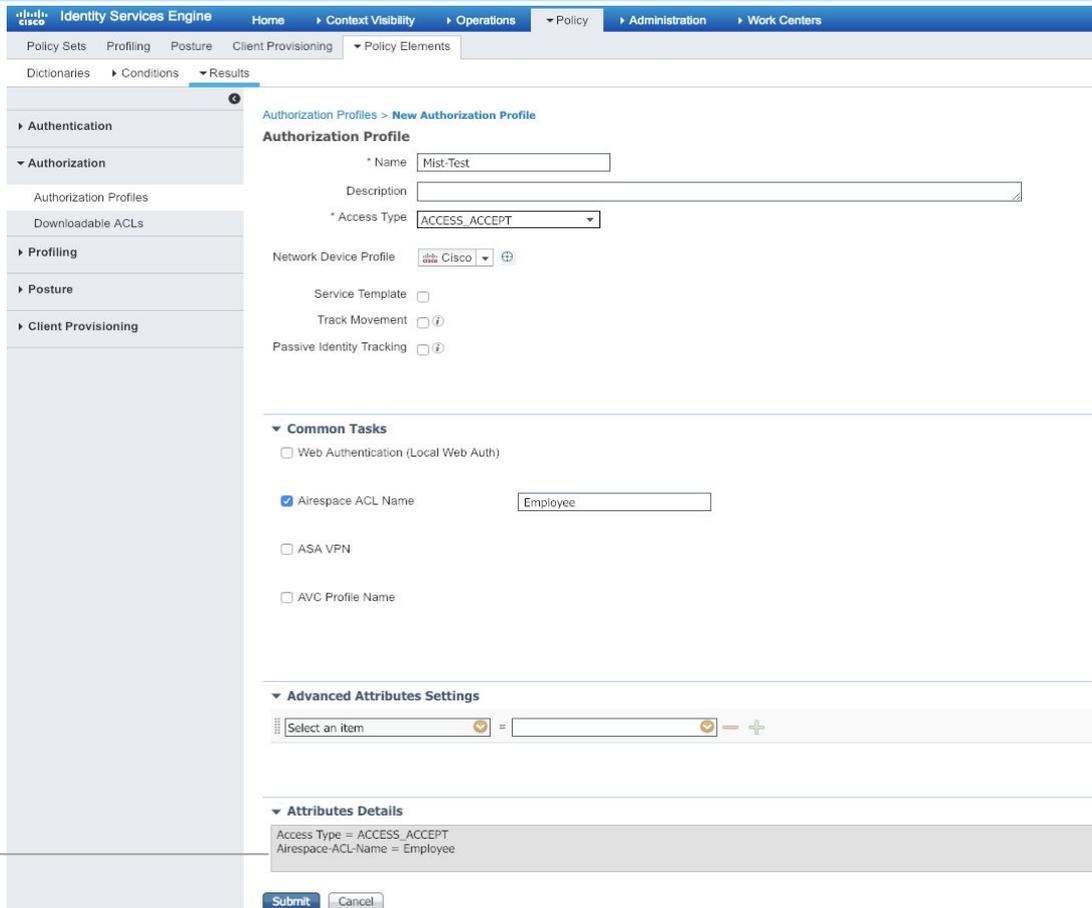
Role-Based Policy Enforcement

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



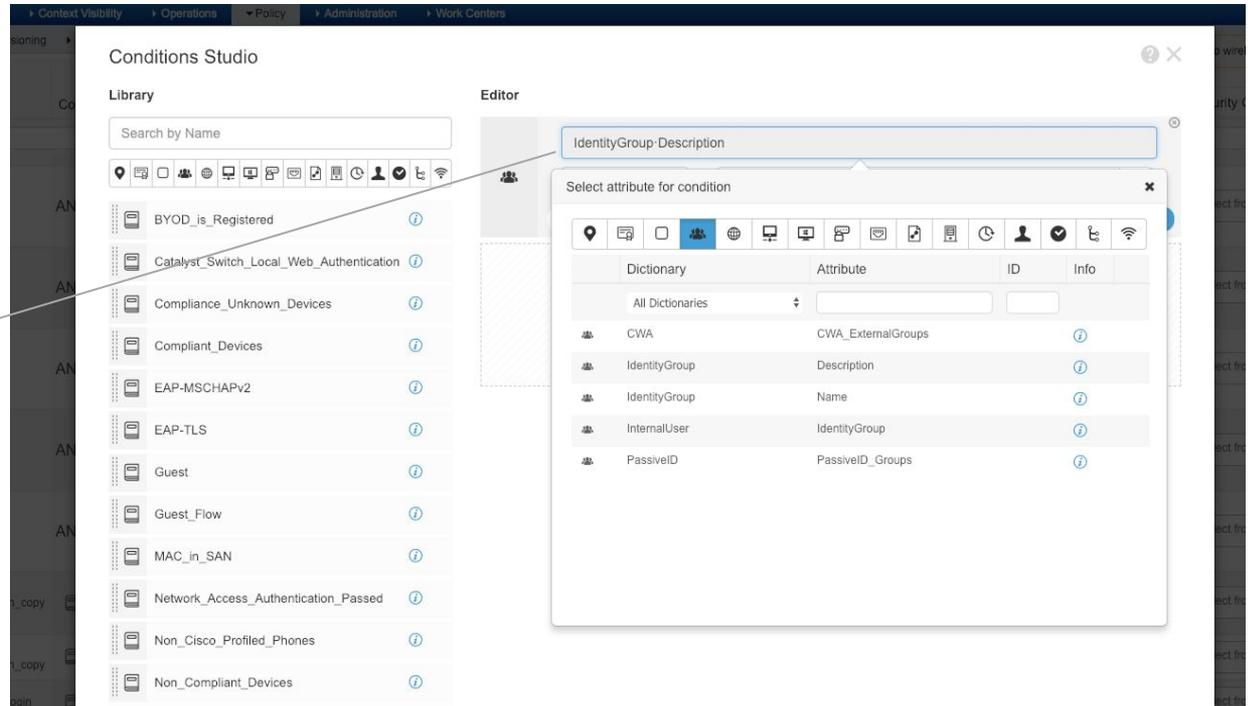
The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes: Policy Sets, Profiling, Posture, Client Provisioning, Policy Elements, Dictionaries, Conditions, and Results. The left sidebar shows a tree view with: Authentication, Authorization (selected), Authorization Profiles, Downloadable ACLs, Profiling, Posture, and Client Provisioning. The main content area is titled "Authorization Profiles > New Authorization Profile" and "Authorization Profile". The form fields are: * Name: Mist-Test; Description: (empty); * Access Type: ACCESS_ACCEPT; Network Device Profile: Cisco; Service Template: (unchecked); Track Movement: (unchecked); Passive Identity Tracking: (unchecked). The "Common Tasks" section includes: Web Authentication (Local Web Auth) (unchecked), Airespace ACL Name: Employee (checked), ASA VPN (unchecked), and AVC Profile Name (unchecked). The "Advanced Attributes Settings" section shows a dropdown menu with "Select an item" and a plus sign. The "Attributes Details" section shows: Access Type = ACCESS_ACCEPT and Airespace-ACL-Name = Employee. At the bottom are "Submit" and "Cancel" buttons.

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

		Employee_Policy	 Employee	<input type="text" value="Mist-Test"/> 	Select from list  	
		Basic_Authenticated_Access	 Network_Access_Authentication_Passed	<input type="text" value="PermitAccess"/> 	Select from list   0	
		Default		<input type="text" value="DenyAccess"/> 	Select from list   0	

Reset

Save

Role-Based Policy Enforcement

Mist Configuration

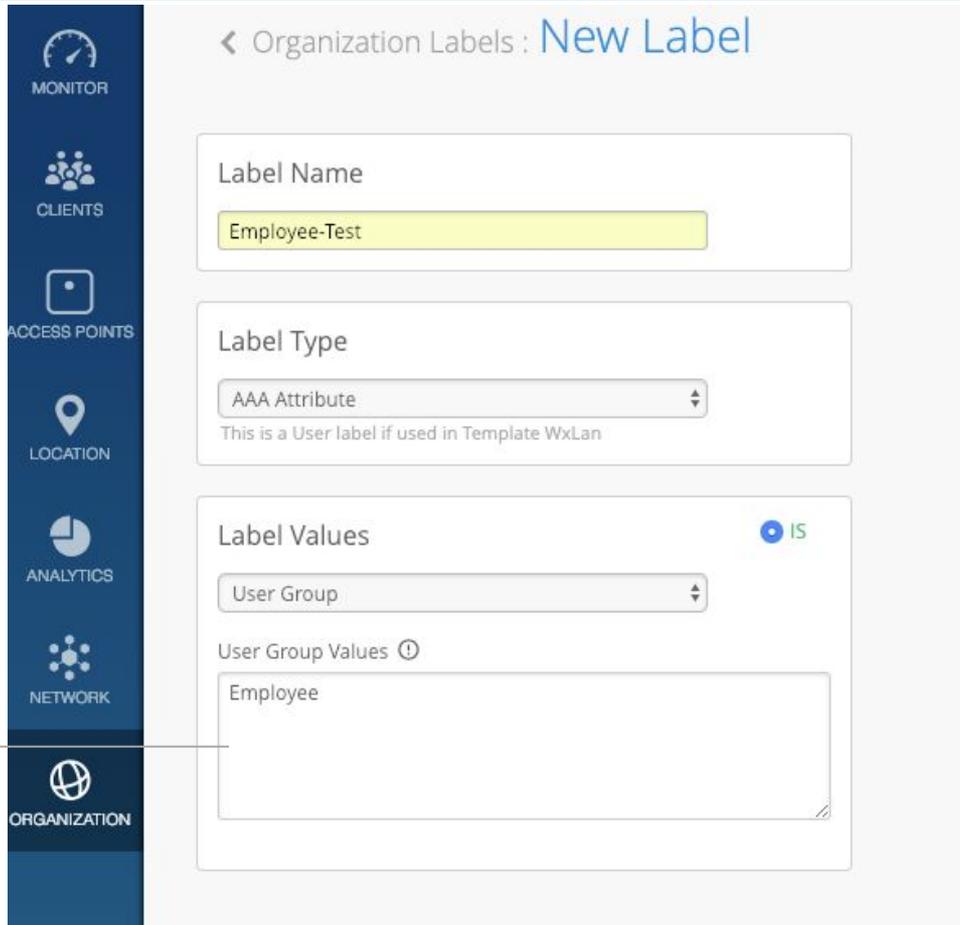
Need to tie the AVP from ISE to WxLAN

1) Configure the Label

- a) Create a label*
- b) Choose Label 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



The screenshot shows the Mist Configuration interface for creating a new label. The left sidebar contains navigation icons for MONITOR, CLIENTS, ACCESS POINTS, LOCATION, ANALYTICS, NETWORK, and ORGANIZATION. The main content area is titled 'Organization Labels : New Label' and contains three sections:

- Label Name:** A text input field containing 'Employee-Test'.
- Label Type:** A dropdown menu set to 'AAA Attribute'. Below it, a note states: 'This is a User label if used in Template WxLan'.
- Label Values:** A dropdown menu set to 'User Group'. To the right of this section is a blue 'IS' icon. Below the dropdown is a section titled 'User Group Values' with an information icon. A text area contains the value 'Employee'.

An arrow points from the text 'The string should be an exact match to the value in the AVP we created in Step 1 on ISE Config' to the 'Employee' value in the 'User Group Values' text area.

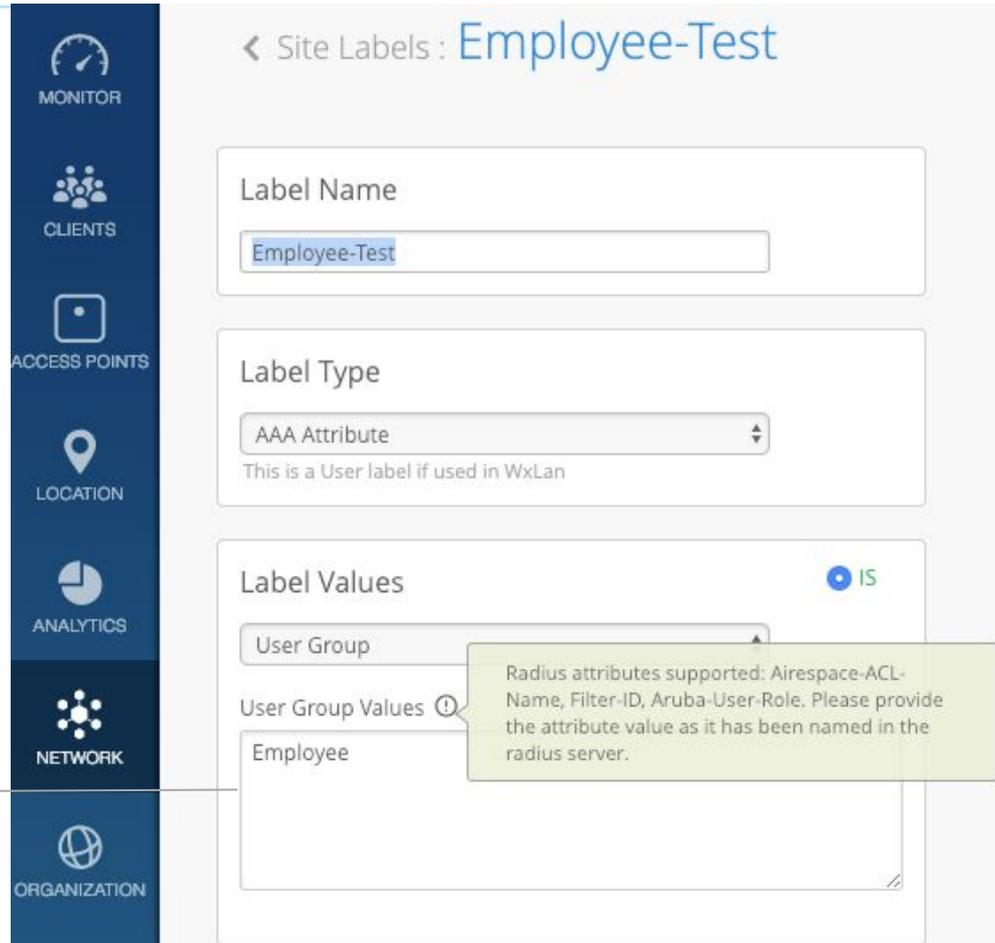
Role-Based Policy Enforcement

Mist Configuration

- 1) Create the Label
 - a) Need to tie the AVP from ISE to WxLAN
 - b) Choose Label 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



The screenshot shows the Mist configuration interface for Site Labels. The breadcrumb is "Site Labels: Employee-Test". The configuration is as follows:

- Label Name:** Employee-Test
- Label Type:** AAA Attribute (This is a User label if used in WxLan)
- Label Values:** User Group (Selected) with a toggle for IS.
- User Group Values:** Employee

A tooltip for the User Group Values field states: "Radius attributes supported: Airespace-ACL-Name, Filter-ID, Aruba-User-Role. Please provide the attribute value as it has been named in the radius server."

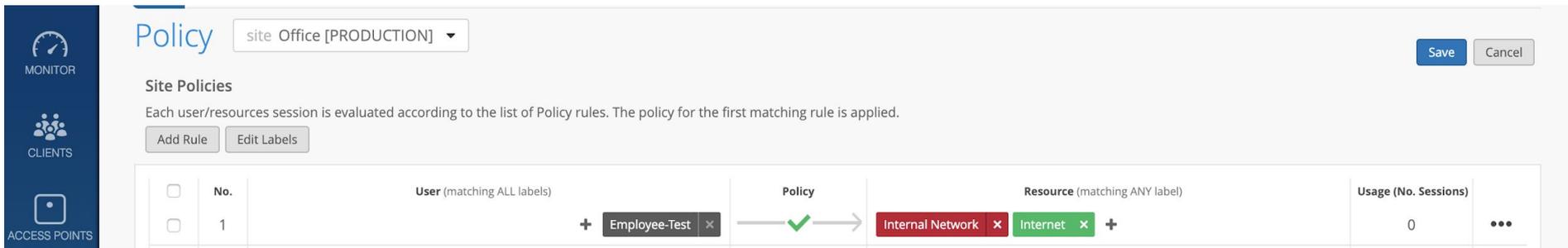
The left sidebar contains navigation icons for MONITOR, CLIENTS, ACCESS POINTS, LOCATION, ANALYTICS, NETWORK, and ORGANIZATION.

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.



The screenshot shows the Mist configuration interface for a Policy. The site is set to "Office [PRODUCTION]". The policy is titled "Site Policies" and is described as "Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied." There are buttons for "Add Rule" and "Edit Labels". The policy rule is displayed in a table with the following columns: No., User (matching ALL labels), Policy, Resource (matching ANY label), and Usage (No. Sessions). The rule has a No. of 1, a User tag of "Employee-Test", a Policy of "allow" (indicated by a green checkmark), and Resources of "Internal Network" (denied, red box) and "Internet" (allowed, green box). The Usage is 0 sessions.

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	+ Employee-Test x	→ ✓ →	Internal Network x Internet x +	0 ...

Thankyou

