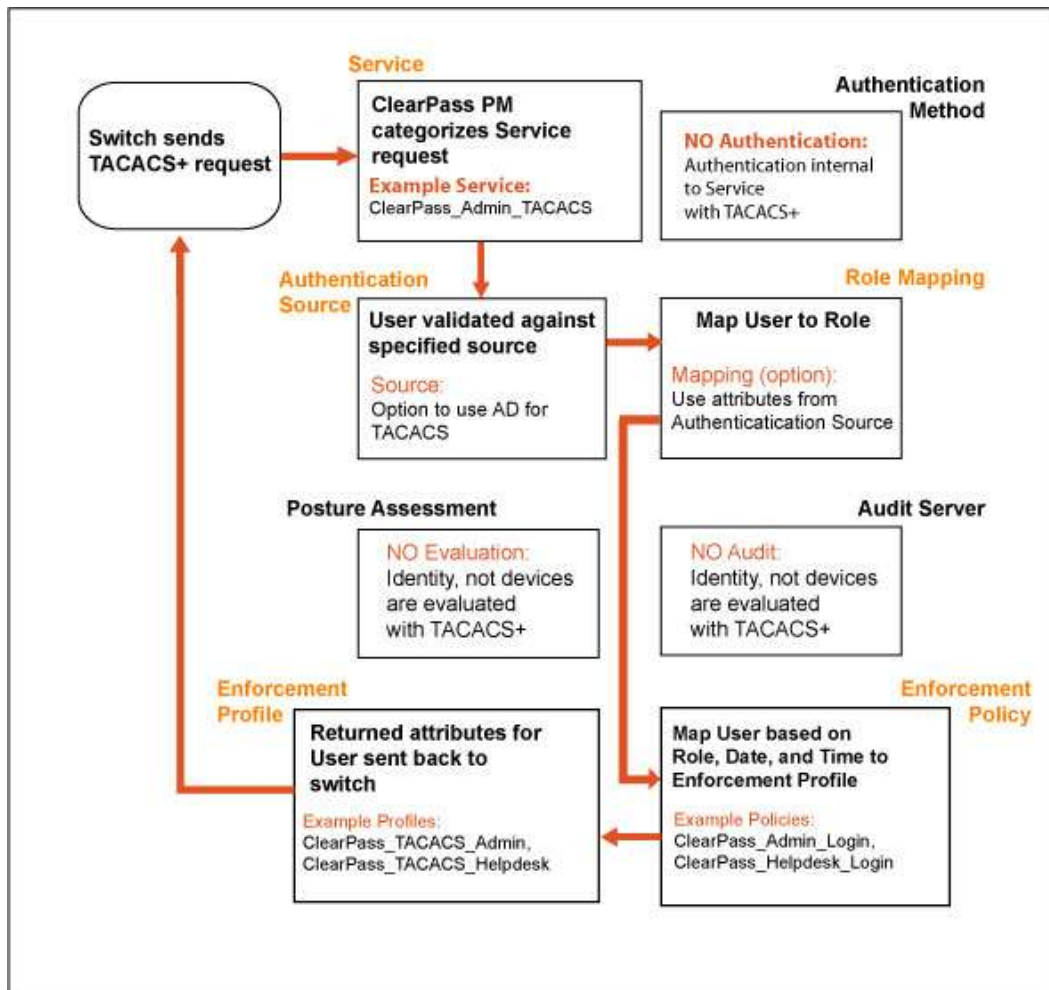


ClearPass Policy Manager: Configuring a TACACS+ Service

Adding this Service supports managed Administrator connections to network access devices via the TACACS+ protocol.

The following illustration highlights the flow of control between TACACS+ and Aruba's Policy Manager.


Figure 1: TACACS+ Connection Flow



1.0 Configuring the Policy Manager TACACS+ Service

Go to the **Configuration » Start Here » Templates » TACACS+ Enforcement** ClearPass Policy Manager admin page to begin.

Start by naming your new Service

Configuration Steps									
<ul style="list-style-type: none">• Enter new Name on appropriate line• Click Next	 <p>The screenshot shows the 'Services' configuration page. The 'Service' tab is active. The 'Type' is 'TACACS+ Enforcement'. The 'Name' is 'TACACS Service'. The 'Description' is empty. The 'Monitor Mode' checkbox is unchecked. Below the form is a 'Service Rule' section with a table for conditions.</p> <table border="1"><thead><tr><th>Type</th><th>Name</th><th>Operator</th><th>Value</th></tr></thead><tbody><tr><td colspan="4">1. Click to add...</td></tr></tbody></table>	Type	Name	Operator	Value	1. Click to add...			
Type	Name	Operator	Value						
1. Click to add...									

2.0 Adding Authentication / Authorization for TACACS+

In this next screen you'll add an Authentication Source from the drop-down list or you can create a new one.

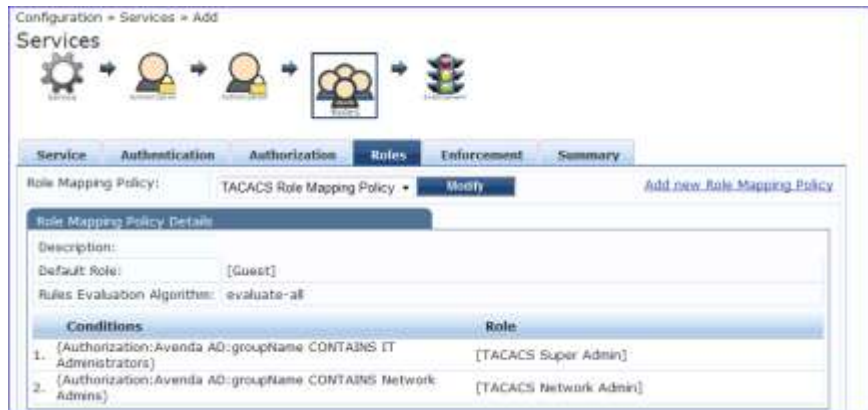
Configuration Steps	
<ul style="list-style-type: none">• Use the Select to Add drop down to add a source (ex: Active Directory where all users are defined)• Click Next• You are now shown the Authorization screen• Click Next to accept defaults	 <p>The screenshot shows the 'Services' configuration page with the 'Authentication' tab selected. The 'Authentication Sources' list contains 'Aravinda AD (Active Directory)'. A context menu is open over the source, showing options: 'Move Up', 'Move Down', 'Remove', 'View Details', and 'Modify'. The 'Strip Username Rules' checkbox is unchecked.</p>

3.0 Assigning User Roles to the TACACS+ Service

This next step allows you to define which roles are provided Admin privileges per your new TACACS+ Service.

Configuration Steps

- Use the **Role Mapping Policy** to select or modify a role for the Service (See **Figure 1** for examples)
- Click **Next**

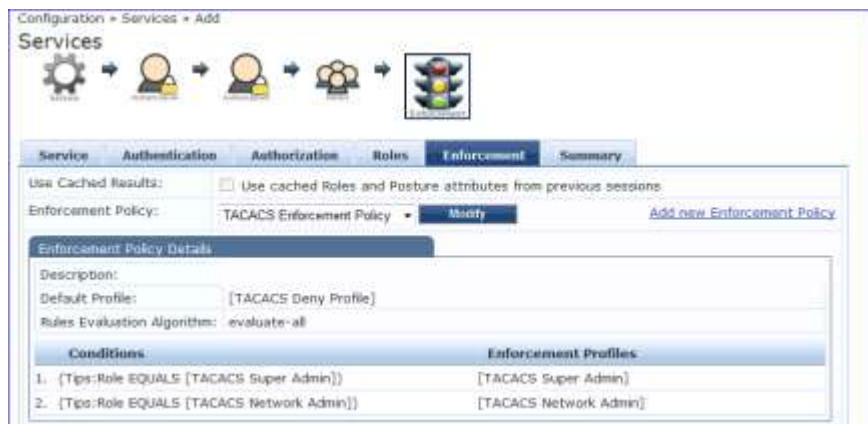


4.0 Mapping User Roles to an Enforcement Policy

This next step allows you to map an Enforcement Policy for the roles that you previously defined.

Configuration Steps

- Select the **Enforcement Policy** you wish to use from the drop down (See **Figure 1** for examples)
- Click **Next**



Completing the Service

Configuration Steps

- Review the contents of your new Service in order to approve or alter any attributes
- Click **Next** to finish

Configuration > Services > Add Services

Services

Service has not been saved

Service Authentication Authorization Roles Enforcement Summary

Service:

Type: TACACS+ Enforcement

Name: TACACS Service

Description:

Monitor Mode: Disabled

Service Rule

Match ALL of the following conditions:

Type	Name	Operator	Value
------	------	----------	-------

Authentication:

Authentication Sources: Avenda AD [Active Directory]

Strip Username Rules: -

Authorization:

Authorization Details: -

Roles:

Role Mapping Policy: TACACS Role Mapping Policy

Enforcement:

Use Cached Results: Disabled

Enforcement Policy: TACACS Enforcement Policy

For Assistance

support@arubanetworks.com or 408.227.4500