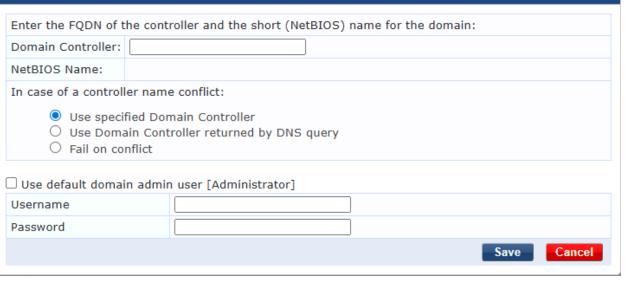
### **Aruba ClearPass Policy Manager with WTI TACACS**

### Step1: Join AD Domain Controller

Join AD Domain

- 1. In the Policy Manager, navigate to Administration > Server Manager > Server Configuration
- 2. Under **AD Domains** section click Join **AD Domain button** and fill in all requirement and click save.



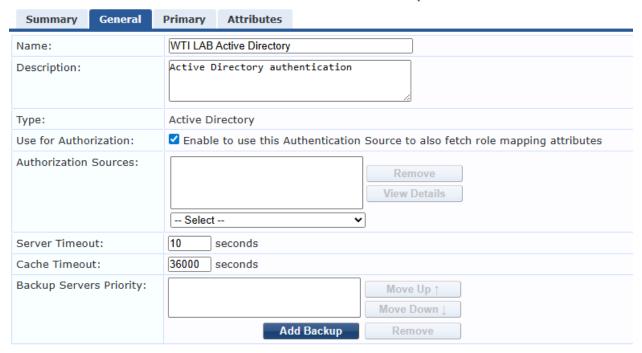
#### Sample page



# **Step 2: Adding Active Directory as an Authentication Source**

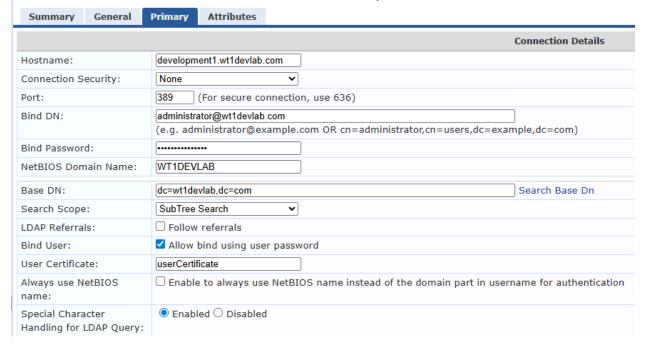
- 1. In the Policy Manager, navigate to **Configuration > Authentication > Sources >** click the **Add** link
- 2. In **General** section under **Type** dropdown select **Active Directory** and fill in all requirements.

# Authentication Sources - WTI LAB Active Directory



3. In **Primary** section, fill in all requirements.

Authentication Sources - WTI LAB Active Directory



# 4. In **Attributes** section, enable any if needed.

Authentication Sources - WTI LAB Active Directory

Sumi	mary General	Primary	Attributes	,									
Specify filter queries used to fetch authentication and authorization attributes													
Filter Name				Attribute Name	Alias Name	Enabled As							
1.	Authentication			distinguishedName	UserDN	-							
				department	Department	-							
				title	Title	-							
				company	company	-							
				memberOf	memberOf	Role							
				telephoneNumber	Phone	-							
				mail	Email	-							
				displayName	Name	-							
				accountExpires	Account Expires	-							
2.	Group			cn	Groups	-							
3.				dNSHostName	HostName	-							
	Machine	operatingSystem	OperatingSystem	-									
				operatingSystemServicePack	OSServicePack	-							
4.	Onboard Device	Owner		memberOf	Onboard memberOf	÷							
5.	Onboard Device	Owner Group	)	cn	Onboard Groups	=							

#### 5. Save

# Summary page

# Authentication Sources - WTI LAB Active Directory

Summary	General	Primary	Attributes				
General:							
Name:		WTI LAB	WTI LAB Active Directory				
Description:		Active Di	Active Directory authentication				
Type:		Active Di	Active Directory				
Use for Autho	rization:	Enabled	Enabled				
Authorization	Sources:	-					
Primary:							
Hostname:		developm	nent1.wt1devla				
Connection Se	ecurity:	None					
Port:		389					
Bind DN:		administr	administrator@wt1devlab.com				
Bind Password:		को को को को को को को को					
NetBIOS Domain Name:		WT1DEVI	LAB				
Base DN:		dc=wt1d	evlab,dc=com				
Search Scope	:	SubTree	Search				
Bind User:		true	true				
User Certificate:		userCerti	userCertificate				
Special Character Handling for LDAP Query:		Enabled :	Enabled				
Attributes:							
Filters:		2. (distin 3. (&(sAN 4. (&(sAN	MAccountName guishedName= MAccountName MAccountName				

5. (distinguishedName=%{Onboard memberOf})

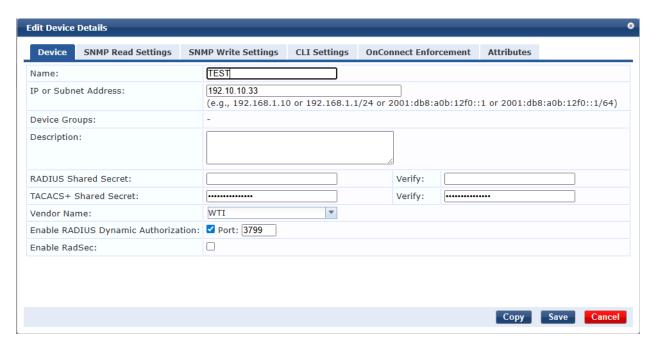
# **Step 3: Import WTI TACACS+ Services**

1. In the Policy Manager, navigate to **Administration > Dictionaries > TACACS+ Services > Import.** 



# **Step 4: Add Devices**

- 1. In the Policy Manager, navigate to **Configuration > Network > Devices >** click the **Add** link
- 2. In **Device** section:
  - Name: {Name your device}
  - IP or Subnet Address: {Device IP Address or subnet Address}
  - TACACS+ Shared Secret: {your TACACS shared secret}
  - Vendor Name: WTI
  - Enable RADIUS Dynamic Authorization: check port 3799
- 3. Save



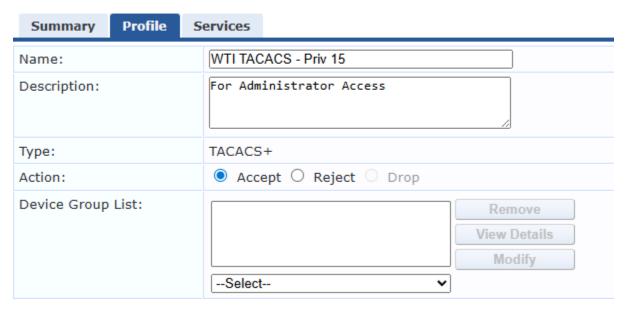
# **Step 5: Create WTI TACACS Profiles**

- 1. In the Policy Manager, navigate to Configuration > Enforcement > Profiles > click the Add link
- 2. In Profile section:

Template: TACACS+ Based EnforcementName: {Name your tacacs profile}

Type: TACACS+Action: Accept

# Enforcement Profiles - WTI TACACS - Priv 15



#### 3. In **Services** section:

# **For Administrator Access Level**

Privilege Level: 15 (Privileged)Selected Services: WTI:TCP

# **Service Attributes**

Type: WTI:TCPName: priv-lvlValue: 15

## For user Access Level

Type: WTI:TCPName: priv-lvlValue: 5

#### Enforcement Profiles - WTI TACACS - Priv 15



# Summary page

## Enforcement Profiles - WTI TACACS - Priv 15

Summary Profile S	ervices									
Profile:										
Name:	WTI TACACS - Priv 15									
Description:	For Administrator Access									
Type:	TACACS+									
Action:	Accept									
Device Group List:	-									
Services:										
Privilege Level:	15									
Selected Services:	1. WTI:TCP									
Authorize Attribute Status:	ADD									
Custom Services:	-									
	Service Attributes									
Туре	Name	=	Value							
1. WTI:TCP	priv-lvl	=	15							

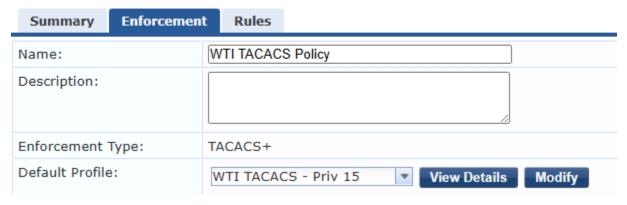
### **Step 6: Create WTI TACACS+ Policies**

- 1. In the Policy Manager, navigate to Configuration > Enforcement > Policies > Click the Add link
- 2. In **Enforcement** section:

Name: {Name your policies}Enforcement Type: TACACS+

• **Default Profile:** {select your Tacacs profile that you created in step 5}

# Enforcement Policies - WTI TACACS Policy



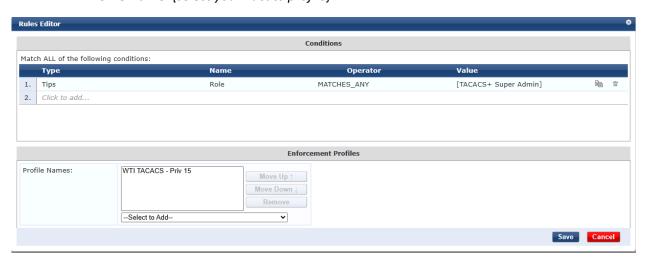
## 3. In Rules section > Add Rule

For Tips:

Type: TipsName: Role

Operator: MATCHES\_ANYValue: {TACACS+ Super Admin}

• Profile Name: {select your Tacacs profile}



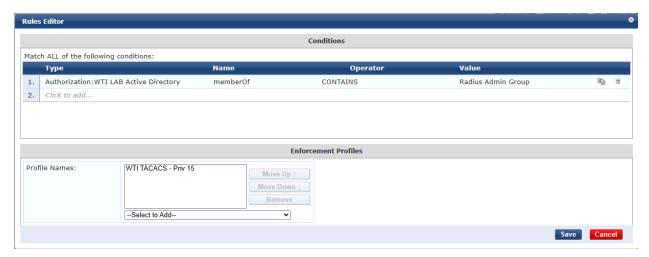
#### For Authorization:

• Type: Authorization: {Your domain active directory}

Name: memberOfOperator: CONTAINS

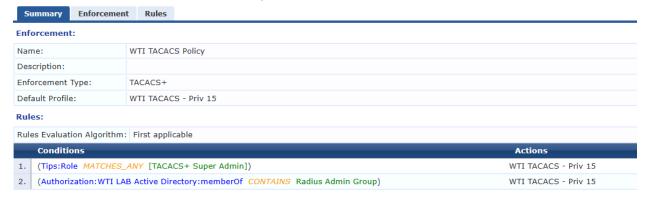
• Value: {Your TACACS Admin Group}

• Profile Name: {select your tacacs profile}



### Summary page

### Enforcement Policies - WTI TACACS Policy



# **Step 7: Create WTI TACACS+ Services**

- 1. In Policy Manager, navigate to **Configuration > Services >** Click the **Add** link
- 2. In Service section:

• **Type:** TACACS+ Enforcement

• Name: {Name your tacacs service}

### **Under Service Rule:**

Type: Connection
 Name: Protocol
 Operator: Equals
 Value: TACACS

#### Services - WTI TACACS Service



### 3. In **Authentication** section:

• Authentication Sources: {Your Active Directory}

# Services - WTI TACACS Service



### 4. In **Enforcement** section:

Authentication Sources: WTI LAB Active Directory [Active Directory]

Disabled

Enforcement Policy: WTI TACACS Policy

Strip Username Rules:

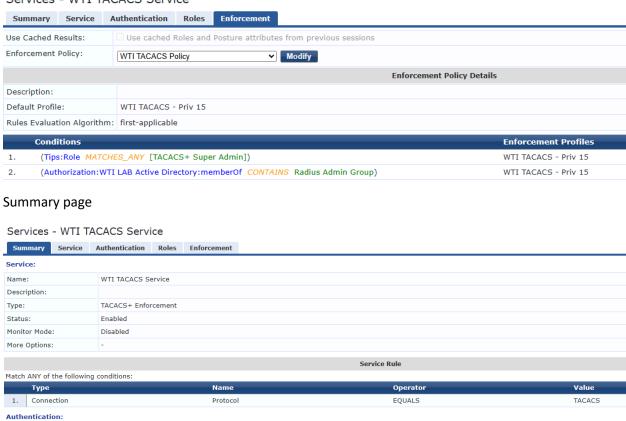
Role Mapping Policy:

Enforcement:

Use Cached Results:

• Enforcement Policy: {Select Your WTI TACACS Policy}

### Services - WTI TACACS Service



# **WTI TACACS Configuration**

1. From CLI, enter /N and select 28 for TACACS.

```
Enter: #<CR> to change,
      <ESC> to exit and save configuration ... 28
TACACS: [Shared]
   Enable:
1.
                               0n
Primary host/address:
                               192.10.10.245
Secondary host/address:
4. Secret Word:
                               (defined)
Fallback Timer:
                               15 Sec
                               On (All failures)
6. Fallback Local:
7. Authentication Port:
Default User Access:
                               0ff
9. Account Management Module:
                              Enabled
10 Session Management Module: Disabled
11. Service Name:
                               wti
12. Debug:
                               0ff
13. Ping Test
Enter: #<CR> to change,
      <ESC> to return to previous menu ...
```