

Aruba ClearPass Policy Manager with WTI TACACS

Step1: Join AD Domain Controller

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.

Join AD Domain

Enter the FQDN of the controller and the short (NetBIOS) name for the domain:

Domain Controller:

NetBIOS Name:

In case of a controller name conflict:

☒ Use specified Domain Controller

☐ Use Domain Controller returned by DNS query

☐ Fail on conflict

☐ Use default domain admin user [Administrator]

Username

Password

Save

Cancel

Sample page

AD Domains:			Join AD Domain
Domain Controller	NetBIOS Name	Password Servers	Action
1. WT1DEVLAB.COM	WT1DEVLAB	-	Leave AD Domain

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

Summary	General	Primary	Attributes
Name:	<input type="text" value="WTI LAB Active Directory"/>		
Description:	<input type="text" value="Active Directory authentication"/>		
Type:	Active Directory		
Use for Authorization:	<input checked="" type="checkbox"/> Enable to use this Authentication Source to also fetch role mapping attributes		
Authorization Sources:	<div><input type="text"/> -- Select --</div> <div><button>Remove</button> <button>View Details</button></div>		
Server Timeout:	<input type="text" value="10"/> seconds		
Cache Timeout:	<input type="text" value="36000"/> seconds		
Backup Servers Priority:	<div><input type="text"/> <div><button>Move Up ↑</button> <button>Move Down ↓</button> <button>Add Backup</button> <button>Remove</button></div></div>		

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

Authentication Sources - WTI LAB Active Directory

Summary	General	Primary	Attributes
Connection Details			
Hostname:	<input type="text" value="development1.wt1devlab.com"/>		
Connection Security:	<input type="text" value="None"/>		
Port:	<input type="text" value="389"/> (For secure connection, use 636)		
Bind DN:	<input type="text" value="administrator@wt1devlab.com"/> (e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)		
Bind Password:	<input type="password" value="....."/>		
NetBIOS Domain Name:	<input type="text" value="WT1DEVLAB"/>		
Base DN:	<input type="text" value="dc=wt1devlab,dc=com"/> Search Base Dn		
Search Scope:	<input type="text" value="SubTree Search"/>		
LDAP Referrals:	<input type="checkbox"/> Follow referrals		
Bind User:	<input checked="" type="checkbox"/> Allow bind using user password		
User Certificate:	<input type="text" value="userCertificate"/>		
Always use NetBIOS name:	<input type="checkbox"/> Enable to always use NetBIOS name instead of the domain part in username for authentication		
Special Character Handling for LDAP Query:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		

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

Authentication Sources - WTI LAB Active Directory

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

5. Save

Summary page

Authentication Sources - WTI LAB Active Directory

Summary	General	Primary	Attributes
---------	---------	---------	------------

General:

Name:	WTI LAB Active Directory
Description:	Active Directory authentication
Type:	Active Directory
Use for Authorization:	Enabled
Authorization Sources:	-

Primary:

Hostname:	development1.wt1devlab.com
Connection Security:	None
Port:	389
Bind DN:	administrator@wt1devlab.com
Bind Password:	*****
NetBIOS Domain Name:	WT1DEVLAB
Base DN:	dc=wt1devlab,dc=com
Search Scope:	SubTree Search
Bind User:	true
User Certificate:	userCertificate
Special Character Handling for LDAP Query:	Enabled

Attributes:

Filters :	1. (&(sAMAccountName=%{Authentication:Username}))(objectClass=user)) 2. (distinguishedName=%{memberOf}) 3. (&(sAMAccountName=%{Host:Name}\$)(objectClass=computer)) 4. (&(sAMAccountName=%{Onboard:Owner}))(objectClass=user)) 5. (distinguishedName=%{Onboard memberOf})
-----------	---

Step 3: Import WTI TACACS+ Services

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

TACACS+ Service Dictionary Attributes				
Display Name:		WTI:TCP		
#	Name	Display Name	Type	Allowed Values
1.	priv-lvl	Privilege level	Unsigned32	-

Close

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

Edit Device Details			
Device	SNMP Read Settings	SNMP Write Settings	CLI Settings
Name:	<input type="text" value="TEST"/>		
IP or Subnet Address:	<input type="text" value="192.10.10.33"/> <small>(e.g., 192.168.1.10 or 192.168.1.1/24 or 2001:db8:a0b:12f0::1 or 2001:db8:a0b:12f0::1/64)</small>		
Device Groups:	-		
Description:	<div></div>		
RADIUS Shared Secret:	<input type="text"/>	Verify:	<input type="text"/>
TACACS+ Shared Secret:	<input type="text" value="....."/>	Verify:	<input type="text" value="....."/>
Vendor Name:	<input type="text" value="WTI"/>		
Enable RADIUS Dynamic Authorization:	<input checked="" type="checkbox"/> Port: <input type="text" value="3799"/>		
Enable RadSec:	<input type="checkbox"/>		

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 Enforcement*
 - **Name:** *{Name your tacacs profile}*
 - **Type:** *TACACS+*
 - **Action:** *Accept*

Enforcement Profiles - WTI TACACS - Priv 15

Summary	Profile	Services
Name:	<input type="text" value="WTI TACACS - Priv 15"/>	
Description:	<div>For Administrator Access</div>	
Type:	TACACS+	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	<div></div> <div>--Select--</div>	<input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/>

3. In **Services** section:

For Administrator Access Level

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

Service Attributes

- **Type:** WTI:TCP
- **Name:** priv-lvl
- **Value:** 15

For user Access Level

- **Type:** WTI:TCP
- **Name:** priv-lvl
- **Value:** 5

Enforcement Profiles - WTI TACACS - Priv 15

Summary	Profile	Services
Privilege Level:	15 (Privileged)	
Selected Services:	WTI:TCP <div>Remove</div> --Select--	
Authorize Attribute Status:	ADD	
Custom Services:	To add new TACACS+ services / attributes, upload the modified dictionary xml - Update TACACS+ Services Dictionary	
Service Attributes		
Type	Name	= Value
1. WTI:TCP	priv-lvl	= 15
2. Click to add...		

Summary page

Enforcement Profiles - WTI TACACS - Priv 15

Summary	Profile	Services
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		
Type	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

Summary	Enforcement	Rules
Name:	<input type="text" value="WTI TACACS Policy"/>	
Description:	<div></div>	
Enforcement Type:	TACACS+	
Default Profile:	<input type="text" value="WTI TACACS - Priv 15"/>	View Details Modify

3. In **Rules** section > **Add Rule**



For Tips:

- **Type:** Tips
- **Name:** Role
- **Operator:** MATCHES_ANY
- **Value:** {TACACS+ Super Admin}
- **Profile Name:** {select your Tacacs profile}

Rules Editor

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value	
1.	Tips	Role	MATCHES_ANY	[TACACS+ Super Admin]	 
2.	Click to add...				

Enforcement Profiles

Profile Names:

[Move Up ↑](#)

[Move Down ↓](#)

[Remove](#)

--Select to Add--

[Save](#) [Cancel](#)



For Authorization:

- **Type:** Authorization: {Your domain active directory}
- **Name:** memberOf
- **Operator:** CONTAINS
- **Value:** {Your TACACS Admin Group}
- **Profile Name:** {select your tacacs profile}

Rules Editor

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value	
1.	Authorization:WTI LAB Active Directory	memberOf	CONTAINS	Radius Admin Group	 
2.	Click to add...				

Enforcement Profiles

Profile Names:

WTI TACACS - Priv 15

Move Up ↑

Move Down ↓

Remove

--Select to Add--

Save

Cancel

Summary page

Enforcement Policies - WTI TACACS Policy

Summary

Enforcement

Rules

Enforcement:

Name:	WTI TACACS Policy
Description:	
Enforcement Type:	TACACS+
Default Profile:	WTI TACACS - Priv 15

Rules:

Rules Evaluation Algorithm:	First applicable
Conditions	Actions
1. (Tips:Role MATCHES_ANY [TACACS+ Super Admin])	WTI TACACS - Priv 15
2. (Authorization:WTI LAB Active Directory:memberOf CONTAINS Radius Admin Group)	WTI TACACS - Priv 15

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

Summary	Service	Authentication	Roles	Enforcement
Name:	WTI TACACS Service			
Description:				
Type:	TACACS+ Enforcement			
Status:	Enabled			
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization			
Service Rule				
Matches <input checked="" type="radio"/> ANY or <input type="radio"/> ALL of the following conditions:				
Type	Name	Operator	Value	
1. Connection	Protocol	EQUALS	TACACS	
2. Click to add...				

3. In **Authentication** section:

- **Authentication Sources:** *{Your Active Directory}*

Services - WTI TACACS Service

Summary	Service	Authentication	Roles	Enforcement
Authentication Sources:	<div>WTI LAB Active Directory [Active Directory]</div> <div><div>Move Up ↑</div><div>Move Down ↓</div><div>Remove</div><div>View Details</div><div>Modify</div></div> <div>--Select to Add--</div>			
Strip Username Rules:	<input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes			

4. In **Enforcement** section:

- Enforcement Policy: *{Select Your WTI TACACS Policy}*

Services - WTI TACACS Service

Summary	Service	Authentication	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	WTI TACACS Policy Modify			
Enforcement Policy Details				
Description:				
Default Profile:	WTI TACACS - Priv 15			
Rules Evaluation Algorithm:	first-applicable			
Conditions		Enforcement Profiles		
1.	(Tips:Role MATCHES_ANY [TACACS+ Super Admin])			WTI TACACS - Priv 15
2.	(Authorization:WTI LAB Active Directory:memberOf CONTAINS Radius Admin Group)			WTI TACACS - Priv 15

Summary page

Services - WTI TACACS Service

Summary	Service	Authentication	Roles	Enforcement
Service:				
Name:	WTI TACACS Service			
Description:				
Type:	TACACS+ Enforcement			
Status:	Enabled			
Monitor Mode:	Disabled			
More Options:	-			
Service Rule				
Match ANY of the following conditions:				
Type	Name	Operator	Value	
1.	Connection Protocol	EQUALS	TACACS	
Authentication:				
Authentication Sources:	WTI LAB Active Directory [Active Directory]			
Strip Username Rules:	-			
Roles:				
Role Mapping Policy:	-			
Enforcement:				
Use Cached Results:	Disabled			
Enforcement Policy:	WTI TACACS Policy			

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]
```

```
1.  Enable:                               On  
2.  Primary host/address:                 192.10.10.245  
3.  Secondary host/address:  
4.  Secret Word:                         (defined)  
5.  Fallback Timer:                       15 Sec  
6.  Fallback Local:                       On (All failures)  
7.  Authentication Port:                  49  
8.  Default User Access:                  Off  
9.  Account Management Module:            Enabled  
10. Session Management Module:            Disabled  
11. Service Name:                         wti  
12. Debug:                               Off  
13. Ping Test
```

```
Enter: #<CR> to change,  
      <ESC> to return to previous menu ... |
```