

## TACACS with Cisco ISE

### Overview:

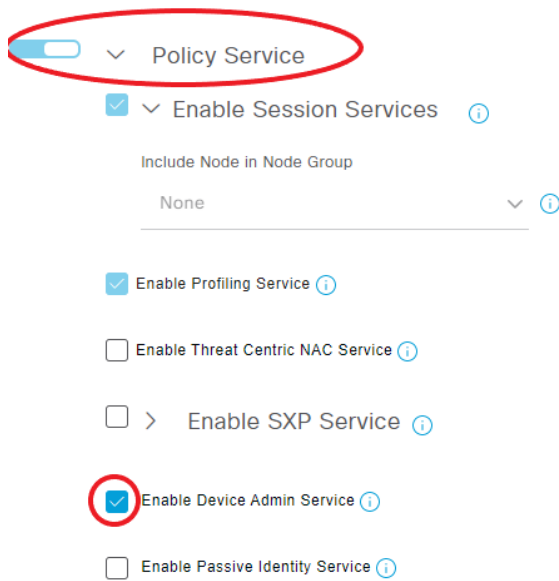
This document describes the steps on how to add WTI unit to Cisco ISE 3.1 for TACACS administration and provide privilege levels from the server.

### Step 1: Enable Device Admin Services:

- Go to **Administration > Deployment**. From there select the node you want to enable the service of in the left-hand menu.



- This should load the **General Settings** tab on the right-hand side. Scroll down to **Policy Service** and enable it. Check the box next to **Device Admin Services**.



## Step 2: Create Network Device Group

- Navigate to **Administration > Network Device Groups**. Check box next to the **All Device Types** and click on **+Add**.

### Network Device Groups

All Groups Choose group ▾

Refresh + Add Duplicate Edit Trash

<input type="checkbox"/>	Name
<input checked="" type="checkbox"/>	All Device Types
<input type="checkbox"/>	WTI-Tech Support
<input type="checkbox"/>	All Locations
<input type="checkbox"/>	> Is IPSEC Device

- This should pop a window asking to **Add Group**. Fill one out for each Device Type that you would like to add.

Add Group

Name\*

Description












Parent Group\*  
All Device Types\*

Cancel Save


### Step 3: Add Network Device

- Navigate to **Administration > Network Devices**. Click add and fill out all the fields with an asterisk next to them. Select the Network device group we created as Device type.

#### Network Devices

Name	WTI-Unit
Description	WTI TACACS
<hr/>	
 IP Address	* IP : 10.1.1.1 / 32 
<hr/>	
Device Profile	 WTI  
Model Name	
Software Version	
<hr/>	
Network Device Group	
Device Type	WTI-Tech Support  <a href="#">Set To Default</a>
IPSEC	Is IPSEC Device  <a href="#">Set To Default</a>
Location	All Locations  <a href="#">Set To Default</a>
WTI	WTI  <a href="#">Set To Default</a>

- Go to **TACACS Authentication Settings** and type the **Shared Secret**. Select **Enable Single Connect Mode** and the **TACACS Draft Compliance Single Connect Support**.

 TACACS Authentication Settings

Shared Secret ..... [Show](#)

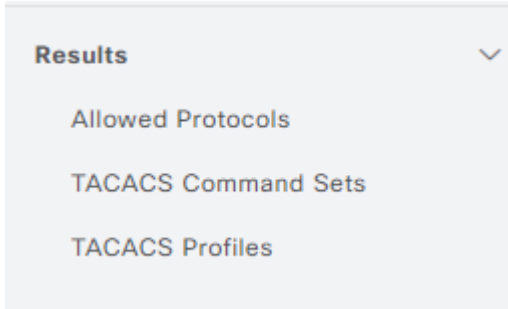
Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

#### Step 4: TACACS Profiles and TACACS Command Sets

- To configure the profile, navigate to **Work Centers > Policy Elements**. On the left-hand side select **Results** and click the dropdown arrow.



- Select TACACS Profiles and click Add. Below is the profile for Admin level access with the privilege level 15.

Name  
WTI Admin Access

Description  
Profile for the users with priv 15

Task Attribute View    Raw View

#### Common Tasks

Common Task Type    Shell    ▾

<input checked="" type="checkbox"/>	Default Privilege	15	▾	(Select 0 to 15)
<input checked="" type="checkbox"/>	Maximum Privilege	15	▾	(Select 0 to 15)
<input type="checkbox"/>	Access Control List		▾	
<input type="checkbox"/>	Auto Command		▾	
<input type="checkbox"/>	No Escape		▾	(Select true or false)
<input type="checkbox"/>	Timeout		▾	Minutes (0-9999)
<input type="checkbox"/>	Idle Time		▾	Minutes (0-9999)

- **Privilege levels for the different access levels:**

View Only – 0-4

User – 5-9

Superuser – 10-14

Admin – 15

- Add a command set in **TACACS Command Sets** to permit all. Click Add from the top menu and fill out as below:

Name

PermitAllCommnads

Description

Default Command Set

Commands

Permit any command that is not listed below



### Step 5: Create Users and User Groups



- Navigate to **Work Centers > Device Administration > User Identity Groups** to create User Groups.
- Below is the example for the Admin level group:

Identity Group

\* Name WTI-Admin

Description For TACACS Admin users

- Create one group for Admin level access and one group for User level access.

<input type="checkbox"/>	 <b>WTI-Admin</b>	For TACACS Admin users
<input type="checkbox"/>	 <b>WTI-Users</b>	For TACACS Users

- Navigate to **Work Centers > Device Administration > Identities** to create Users.
- Below is the example for User with the Admin level and added to the User Group:

Network Access User

\* Username

Status  Enabled

Email

---

Passwords

Password Type:

Password  Re-Enter Password

\* Login Password

Enable Password

---

User Information

First Name

Last Name

---

User Groups

WTI-Admin

[Save](#)

- Create one User with Admin level access and one User with User level access.

<input type="checkbox"/>	<input checked="" type="checkbox"/> Enabled	 wtiadmin	WTI	Admin	WTI-Admin
<input type="checkbox"/>	<input checked="" type="checkbox"/> Enabled	 wtiuser	WTI	User	WTI-Users

## Step 6: Create Policy Sets for device administration

- Go to **Work Centers > Device Administration > Device Admin Policy Sets** and click ADD. Then, select the + icon and it will open a new window for **Conditions Studio**.

Policy Sets

Status	Policy Set Name	Description	Conditions
	WTI Device	TACACS WTI Policy Set	

## Conditions Studio

Library

Search by Name

No conditions found - reset filters.

Editor

TACACS-User

In

[Set to 'Is not'](#) [Duplicate](#) [Save](#)

[NEW](#) [AND](#) [OR](#)

- Next verify that **Default Device Admin** is selected in Allowed Protocols/Server Sequence. Then select left-hand arrow under View to open the Authentication & Authorization Policy section.

Allowed Protocols / Server Sequence	Hits	Actions	View
Default Device Admin	101		

- Select **Internal Users** under the **Authentication Policy** option.
- In **Authorization Policy**, click on the + icon to add rule. Assign Rule Name, Command sets to PermitAllCommands and Shell Profiles. To add conditions, click on the + icon and provide information as below in the Conditions Studio.

# Conditions Studio

## Library

Search by Name \_\_\_\_\_

- EAP-MSCHAPv2 ⓘ
- EAP-TLS ⓘ
- Guest\_Flow ⓘ
- Network\_Access\_Authentication\_Passed ⓘ

## Editor

InternalUser-IdentityGroup

Equals

Set to 'Is not' Duplicate Save

NEW | AND | OR

- Create rules for both Admin and User level Users.

Authorization Policy (3)

Status	Rule Name	Conditions	Results	
			Command Sets	Shell Profiles
✔	WTI-User	InternalUser-IdentityGroup EQUALS User Identity Groups:WTI-Users	PermitAllCommnads	WTI Priv 5_9 User
✔	WTI-Admin	InternalUser-IdentityGroup EQUALS User Identity Groups:WTI-Admin	PermitAllCommnads	WTI Priv 15 Admin



## Step 7: Configure the TACACS parameters on WTI

- Issue /n command and select option 28 for TACACS Parameters.
- TACACS Parameters:
  1. Enable: On
  2. Primary host/address: **XXX.XXX.XXX.XXX** (Cisco ISE IP Address)
  3. Secondary host/address: (undefined)
  4. Secret Word: xxxx (TACACS Secret work from CISCO ISE)
  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: Enabled
  11. Service Name: wti
  12. Debug: Off
  13. Ping Test
- Note: Account Management Module and Session Management Module should be Enabled.

## Step 8: Verification

- Navigate to **Operations > TACACS > Live Logs** to view. A successful Authentication should look like the following:

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...	Network Devic...
×	▼		Identity		▼Authentication Policy	Authorization Policy	Ise Node	Network Device Ni	▼
Jan 09, 2023 04:29:52.1...	✔		techadmin	Authorizat...		WTI Tech Support >> Admin	CiscoISE	WTI-Jalpa	192.10.10.105
Jan 09, 2023 04:29:52.1...	✔		techadmin	Authentic...	WTI Tech Support >> Default		CiscoISE	WTI-Jalpa	192.10.10.105

- If you see failures in the Live Logs for different Authorization requests, this could be the result of users trying to issue unauthorized commands.