

RADIUS with Cisco ISE

Step 1. Create the Vendor-Specific Attribute

1. Navigate to Policy > Policy Element > Dictionaries > System > Radius > Radius Vendors > Add

The screenshot shows the Cisco ISE interface. The top navigation bar includes 'Cisco ISE' and 'Policy · Policy Elements'. Below this, there are tabs for 'Dictionaries', 'Conditions', and 'Results'. The 'Dictionaries' tab is selected and highlighted with a red box. On the left, a sidebar menu shows 'System' and 'User' categories, with 'System' highlighted by a red box. The main content area is titled 'System Dictionaries' and displays a table of system dictionaries.

Name	Description
<input type="checkbox"/> ACIDEX	Profiler ACIDEX dictionary
<input type="checkbox"/> ACTIVE DIRECTORY_PROBE	Profiler ACTIVE DIRECTORY_PROBE dictionary
<input type="checkbox"/> APIC	Dictionary for APIC
<input type="checkbox"/> CDP	Profiler CDP dictionary
<input type="checkbox"/> CERTIFICATE	Cisco Certificate Dictionary

The screenshot shows the Cisco ISE interface. The left sidebar menu is expanded to show 'Radius' and 'RADIUS Vendors', both highlighted with red boxes. The main content area is titled 'RADIUS Vendors' and features a toolbar with 'Edit', '+ Add', 'Delete', 'Import', and 'Export' buttons. The '+ Add' button is highlighted with a red box. Below the toolbar is a table of RADIUS vendors.

Name	Vendor ID	Description
<input type="checkbox"/> Airespace	14179	Dictionary for Vendor Airespace
<input type="checkbox"/> Alcatel-Lucent	800	Dictionary for Vendor Alcatel-Lucent
<input type="checkbox"/> Aruba	14823	Dictionary for Vendor Aruba
<input type="checkbox"/> Brocade	1588	Dictionary for Vendor Brocade
<input type="checkbox"/> Cisco	9	Dictionary for Vendor Cisco
<input type="checkbox"/> Cisco-BBSM	5263	Dictionary for Vendor Cisco-BBSM
<input type="checkbox"/> Cisco-VPN3000	3076	Dictionary for Vendor Cisco-VPN3000
<input type="checkbox"/> H3C	25506	Dictionary for Vendor H3C
<input type="checkbox"/> HP	11	Dictionary for Vendor HP
<input type="checkbox"/> Juniper	2636	Dictionary for Vendor Juniper
<input type="checkbox"/> Microsoft	311	Dictionary for Vendor Microsoft
<input type="checkbox"/> Motorola-Symbol	388	Dictionary for Vendor Motorola-Symbol
<input type="checkbox"/> Ruckus	25053	Dictionary for Vendor Ruckus
<input type="checkbox"/> WISPr	14122	Dictionary for Vendor WISPr
<input type="checkbox"/> WTI	24496	Dictionary for Vendor WTI

2. The name and the Vendor IDs are to be entered and saved.

Dictionary Name: **WTI**

Vendor ID: **24496**

Policy · Policy Elements

Dictionary Name: **WTI**

Description: Dictionary for Vendor WTI

Vendor ID: **24496**

Vendor Attribute Type Field Length: 1

Vendor Attribute Size Field Length: 1

Submit Cancel

3. Click the saved Radius Vendor and navigate to Dictionary Attributes.

Dictionary Attributes

+ Add Edit Delete

<input type="checkbox"/>	Name	Number	Type	Direction	Description	Predefi...
<input type="checkbox"/>	WTI-Super	41	INT	BOTH		NO

4. Click Add and fill out the Attribute Name, Data Type, Direction and ID and Add allow values for access level.

Attribute Name: **WTI-Super**

Data Type: **INT**

Direction: **BOTH**

ID: **41**

Add allow Values for access level

Name: **Administrator**

Value: **3**

Name: **User**

Value: **1**

Dictionary configuration for **WTI-Super**:

- Attribute Name: WTI-Super
- Description:
- Data Type: INT
- Direction: BOTH
- ID: 41 (0-255)
- Allow Tagging:
- Allow multiple instances of this attribute in a profile:
- Allowed Values:

Name	Value
Administrator	3
User	1

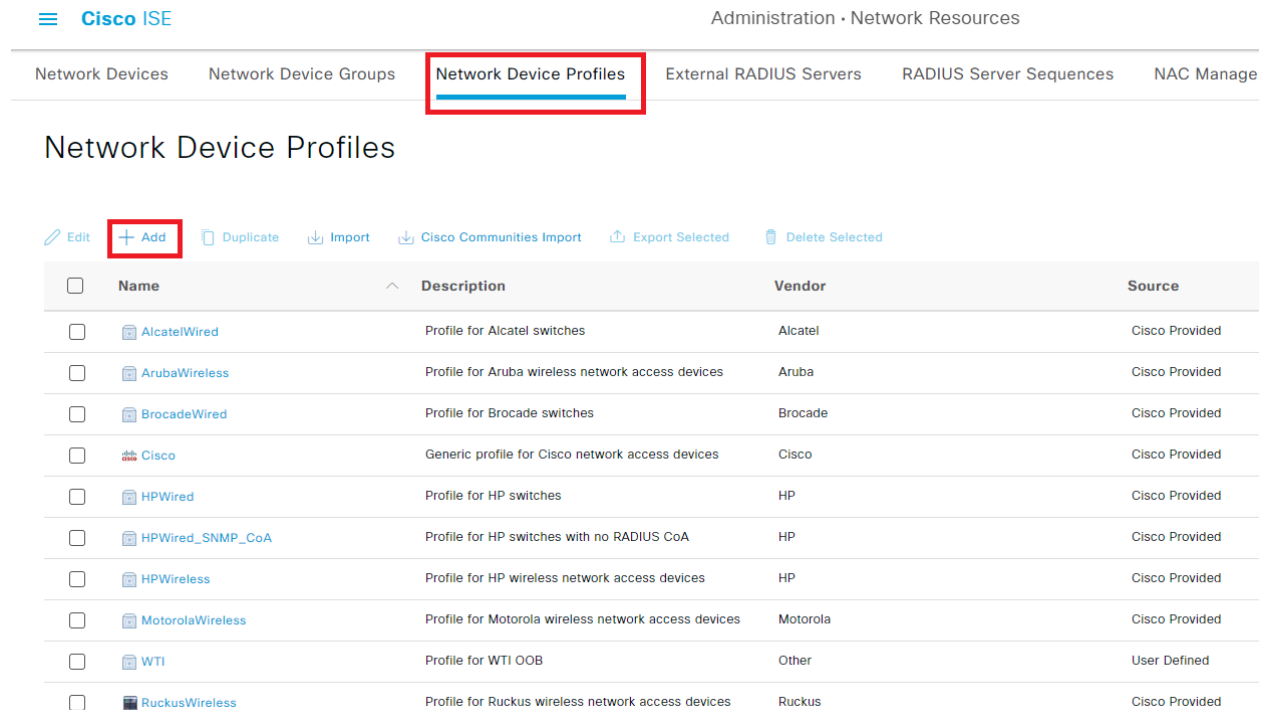
5. Save the attribute.

6. Add other Attributes on the same page if there are multiple Attributes to be added to the same Dictionary.

WTI RADIUS Dictionary <https://ftp.wti.com/InfoCenter/rsa/dictionary/dictionary.wti>

Step 2. Create a Network Device Profile

1. Navigate to **Administration > Network Resources > Network Device Profile > Add**



Cisco ISE Administration - Network Resources

Network Devices | Network Device Groups | **Network Device Profiles** | External RADIUS Servers | RADIUS Server Sequences | NAC Manage

Network Device Profiles

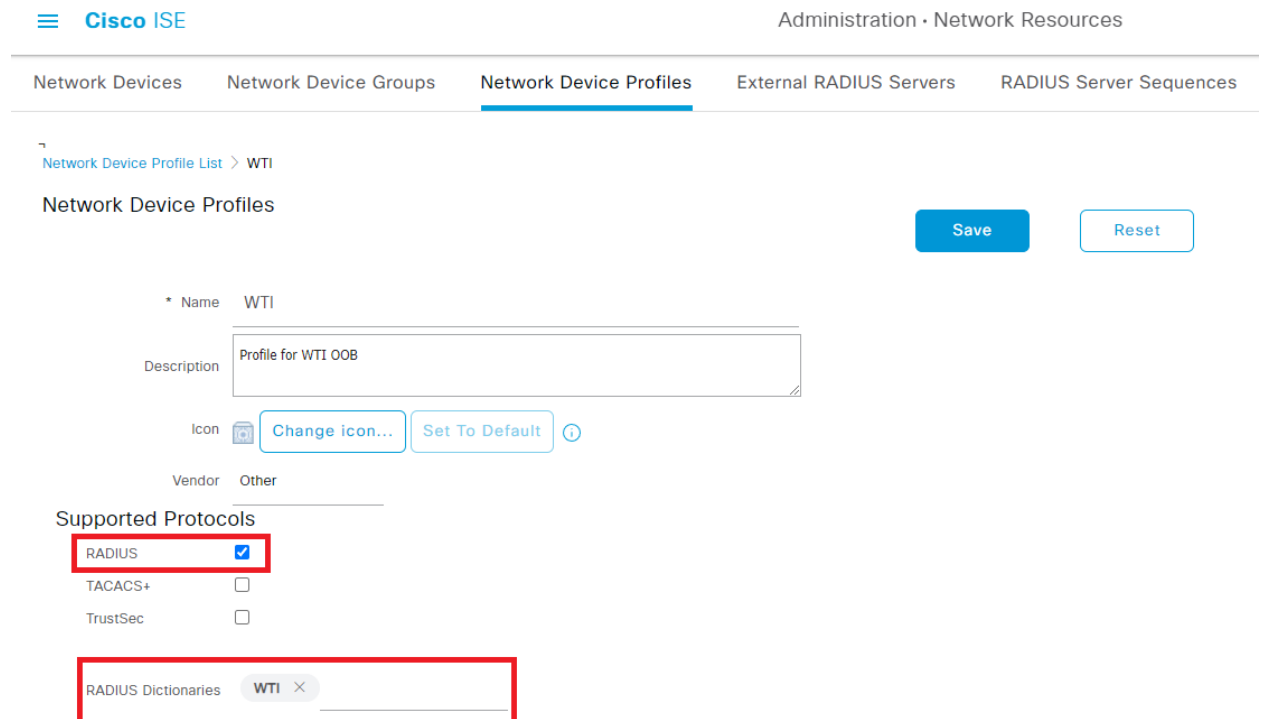
Edit **+ Add** Duplicate Import Cisco Communities Import Export Selected Delete Selected

<input type="checkbox"/>	Name	Description	Vendor	Source
<input type="checkbox"/>	AlcateWired	Profile for Alcatel switches	Alcatel	Cisco Provided
<input type="checkbox"/>	ArubaWireless	Profile for Aruba wireless network access devices	Aruba	Cisco Provided
<input type="checkbox"/>	BrocadeWired	Profile for Brocade switches	Brocade	Cisco Provided
<input type="checkbox"/>	Cisco	Generic profile for Cisco network access devices	Cisco	Cisco Provided
<input type="checkbox"/>	HPWired	Profile for HP switches	HP	Cisco Provided
<input type="checkbox"/>	HPWired_SNMP_CoA	Profile for HP switches with no RADIUS CoA	HP	Cisco Provided
<input type="checkbox"/>	HPWireless	Profile for HP wireless network access devices	HP	Cisco Provided
<input type="checkbox"/>	MotorolaWireless	Profile for Motorola wireless network access devices	Motorola	Cisco Provided
<input type="checkbox"/>	WTI	Profile for WTI OOB	Other	User Defined
<input type="checkbox"/>	RuckusWireless	Profile for Ruckus wireless network access devices	Ruckus	Cisco Provided

2. Give a name and check the box for **RADIUS**.

3. Under the **RADIUS Dictionaries**, select the dictionary created in the previous section.

4. If multiple dictionaries were created for the same type of device, all of them can be selected under **RADIUS Dictionaries**.



Cisco ISE Administration - Network Resources

Network Devices | Network Device Groups | **Network Device Profiles** | External RADIUS Servers | RADIUS Server Sequences

Network Device Profile List > WTI

Network Device Profiles

Save Reset

* Name WTI

Description Profile for WTI OOB

Icon

Vendor Other

Supported Protocols

RADIUS

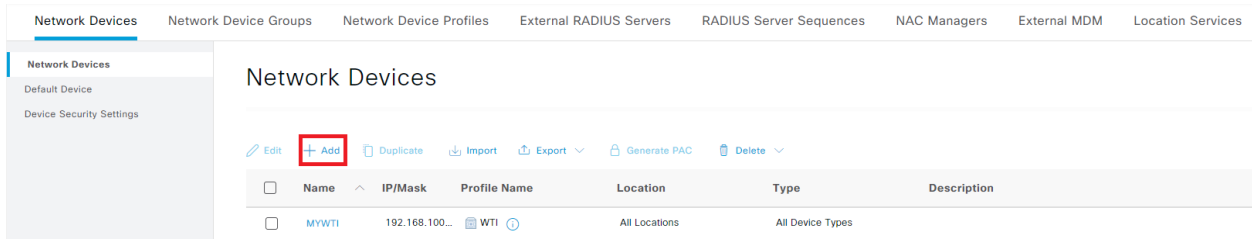
TACACS+

TrustSec

RADIUS Dictionaries **WTI** X

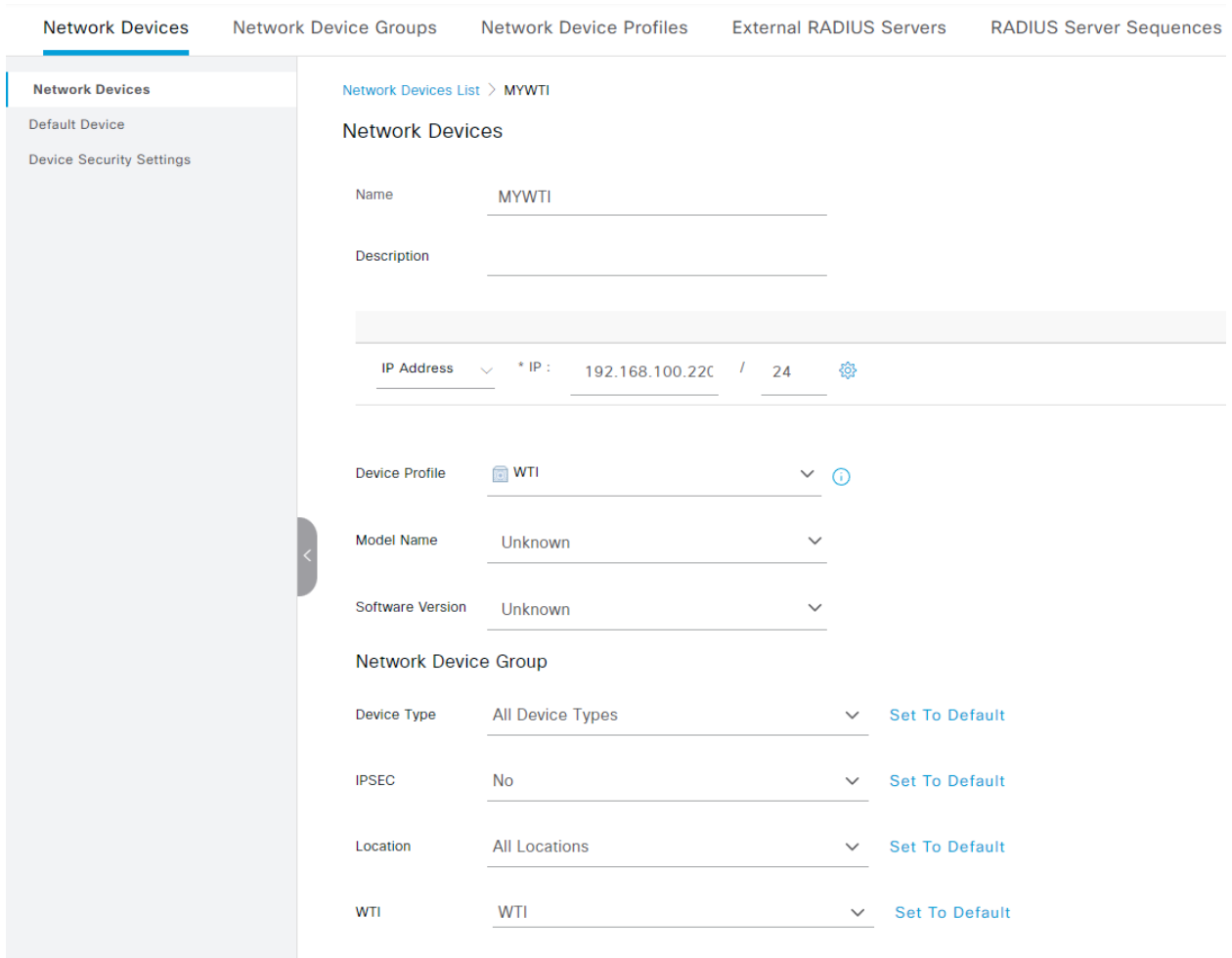
Step 3. Add Network Device on ISE

1. Navigate to **Administration > Network Resources > Network Devices > Add**



2. Give a name and the IP Address

3. The Device Profile can be chosen from the dropdown list to be the one defined. If a profile was not created, the default Cisco can be used as it is.



4. Check Radius Authentication Settings.

5. Enter the **Shared Secret Key** and **save** the device.

v RADIUS Authentication Settings

RADIUS UDP Settings

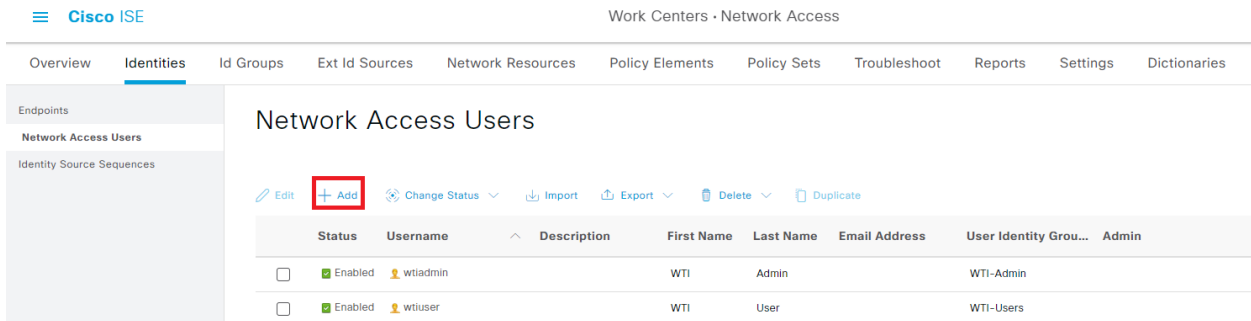
Protocol **RADIUS**

Shared Secret Show

Use Second Shared Secret i

Step 4. Create Network Access Users

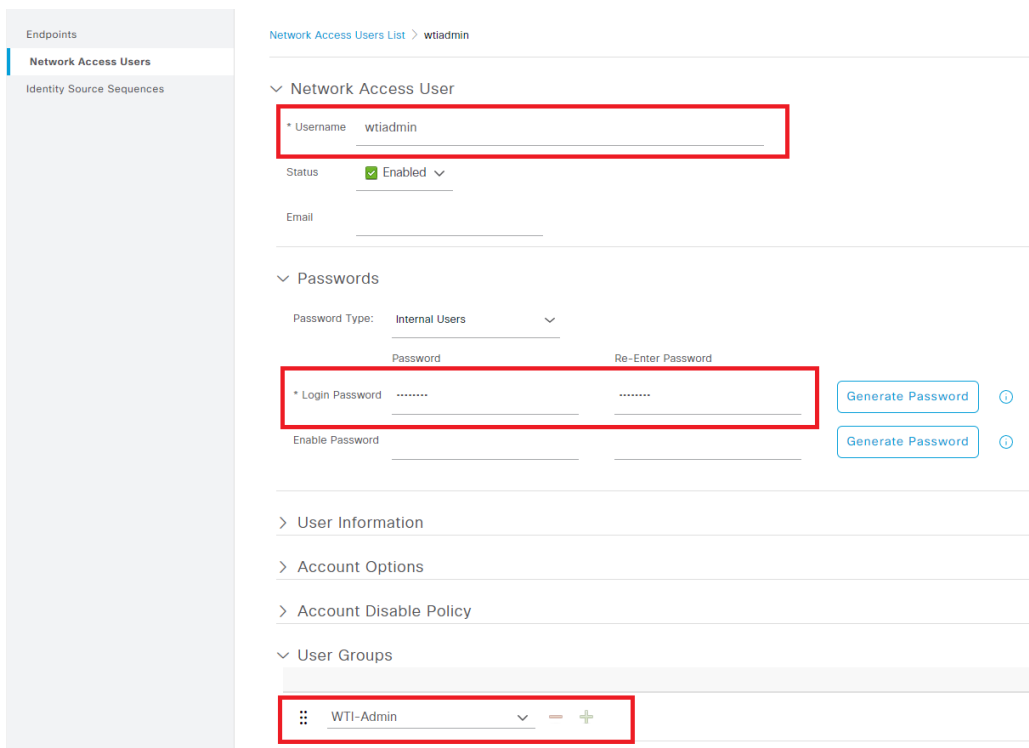
1. Navigate to **Work Centers > Network Access > Identities > Network Access Users > Add**



The screenshot shows the Cisco ISE interface for Network Access Users. The breadcrumb path is "Work Centers > Network Access". The left sidebar shows "Endpoints", "Network Access Users", and "Identity Source Sequences". The main content area is titled "Network Access Users" and contains a table with columns: Status, Username, Description, First Name, Last Name, Email Address, User Identity Group, and Admin. Two users are listed: "wtiadmin" and "wtiuser". A red box highlights the "+ Add" button in the top toolbar.

Status	Username	Description	First Name	Last Name	Email Address	User Identity Group	Admin
<input type="checkbox"/>	Enabled wtiadmin		WTI	Admin		WTI-Admin	
<input type="checkbox"/>	Enabled wtiuser		WTI	User		WTI-Users	

2. Fill out network access, password section and assign User Groups



The screenshot shows the configuration page for a Network Access User named "wtiadmin". The breadcrumb path is "Network Access Users List > wtiadmin". The page is divided into several sections: "Network Access User", "Passwords", "User Information", "Account Options", "Account Disable Policy", and "User Groups". The "Network Access User" section has a red box around the "Username" field containing "wtiadmin". The "Status" is set to "Enabled". The "Passwords" section has a red box around the "Login Password" and "Re-Enter Password" fields, both containing ".....". There are "Generate Password" buttons next to these fields. The "User Groups" section has a red box around a dropdown menu showing "WTI-Admin" with a plus sign to add more groups.

Step 5. Create Authorization Profiles

1. Navigate to Policy > Policy Elements > Results > Authorization Profiles > Add

The screenshot shows the Cisco ISE interface for Policy Elements Results. The left sidebar contains a navigation menu with 'Authorization Profiles' highlighted. The main content area is titled 'Standard Authorization Profiles' and includes a table of existing profiles. The 'Add' button is highlighted with a red box. The 'WTI_Admin' and 'WTI_User' profiles are also highlighted with a red box.

Name	Profile	Description
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure
Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
UDN	Cisco	Default profile used for UDN.
WTI_Admin	WTI	WTI Administrator Access Level
WTI_User	WTI	WTI User Access Level
DenyAccess		Default Profile with access type as Access-Reject
PermitAccess		Default Profile with access type as Access-Accept

2. Create two Authorization Profile. One for WTI_Admin (Administrator access level) and another for WTI_User (User access level).

The screenshot shows the configuration page for the 'WTI_Admin' Authorization Profile. The 'Name' field is 'WTI_Admin', the 'Description' is 'WTI Administrator Access Level', the 'Access Type' is 'ACCESS_ACCEPT', and the 'Network Device Profile' is 'WTI'. The 'Common Tasks' section includes 'ACL' and 'Security Group'. The 'Advanced Attributes Settings' section shows a list of attributes with 'WTI:WTI-Super' and 'Administrator' highlighted. The 'Attributes Details' section shows 'Access Type = ACCESS_ACCEPT' and 'WTI-Super = 3'.

For WTI_Admin

In advanced Attribute Settings

Advanced Attributes Settings

⋮ WTI:WTI-Super = Administrator - +

Attributes Details

Access Type = ACCESS_ACCEPT
WTI-Super = 3

For WTI_User

In Advance Attribute Settings

Advanced Attributes Settings

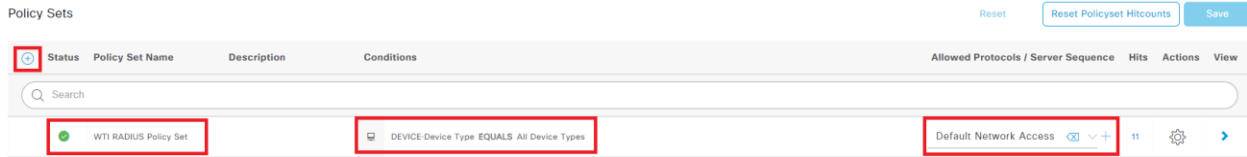
⋮ WTI:WTI-Super = User - +

Attributes Details

Access Type = ACCESS_ACCEPT
WTI-Super = 1

Step 6. Create Policy

1. Navigate to **Policy > Policy Sets > click (+)** to add new policy set.



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	WTI RADIUS Policy Set		DEVICE Device Type EQUALS All Device Types				
				Default Network Access	11		

Policy Set Name: **WTI RADIUS Policy Set**

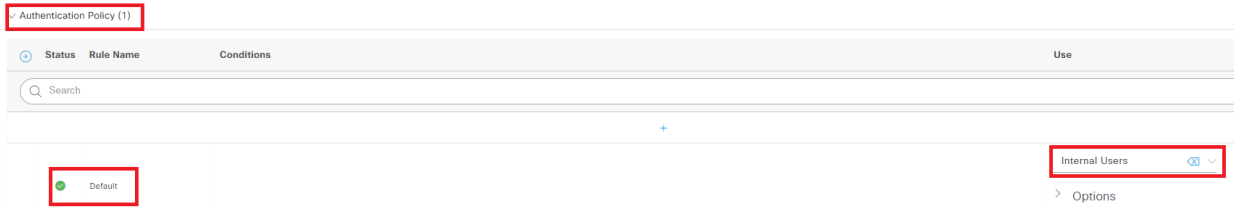
Condition: DEVICE: Device Type **EQUALS** All Device Types

Allowed Protocols: **Default Network Access**

2. Authentication Policy

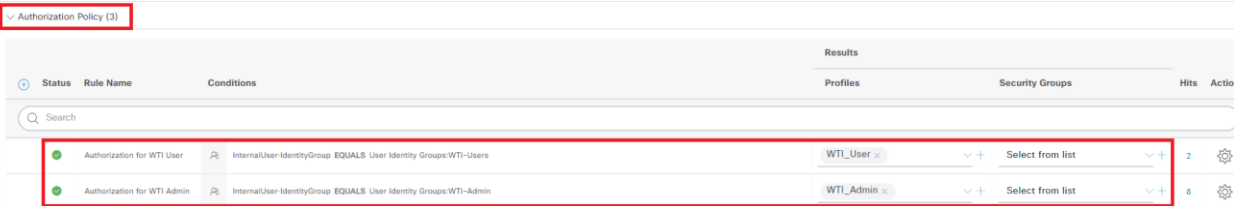
Rule Name: Default

Use: **Internal User**



Status	Rule Name	Conditions	Use
●	Default		Internal Users

3. Authorization Policy – create two authorization policy, one for WTI_Admin and another for WTI_User.



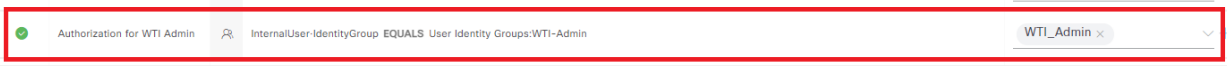
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Action
●	Authorization for WTI User	InternalUser-IdentityGroup EQUALS User Identity Groups:WTI-Users	WTI_User	Select from list	2	
●	Authorization for WTI Admin	InternalUser-IdentityGroup EQUALS User Identity Groups:WTI-Admin	WTI_Admin	Select from list	5	

For WTI_Admin

Rule Name: **Authorization for WTI-Admin**

Condition: Internal User-IdentityGroup **EQUALS** User Identity Groups:WTI-Admin

Profile: **WTI_Admin**



Status	Rule Name	Conditions	Profiles
●	Authorization for WTI Admin	InternalUser-IdentityGroup EQUALS User Identity Groups:WTI-Admin	WTI_Admin

For WTI_User

Rule Name: **Authorization for WTI-User**

Condition: Internal User-IdentityGroup **EQUALS** User Identity Groups:WTI-User

Profile: **WTI_User**



Status	Rule Name	Conditions	Profiles
●	Authorization for WTI User	InternalUser-IdentityGroup EQUALS User Identity Groups:WTI-Users	WTI_User

Overview of Policy

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
●	WTI RADIUS Policy Set		DEVICE Device Type EQUALS All Device Types	Default Network Access

Status	Rule Name	Conditions	Use	Hits	Action
●	Default		Internal Users	11	Options

Status	Rule Name	Conditions	Results	Security Groups	Hits	Action
			Profiles			
●	Authorization for WTI User	InternalUser-IdentityGroup EQUALS User Identity Groups:WTI-Users	WTI_User	Select from list	2	Options
●	Authorization for WTI Admin	InternalUser-IdentityGroup EQUALS User Identity Groups:WTI-Admin	WTI_Admin	Select from list	8	Options

WTI RADIUS Setting

1. Go to /N option 29 for Radius
2. RADIUS Setting

Enable: **ON**

Primary Host/Address IPv4: **XXX.XXX.XXX.XXX** (Cisco ISE IP Address)

Primary Secret word: **xxx** (Radius secret from Cisco ISE)

Fallback Timer: **20**

Fallback Local: **On (All failure)**

Retries: **3**

Authentication Port: **1812**

Accounting Port: **1813**

Default User Access: **OFF**

OneTime Auth: **On**

OneTime Auth Timer: **5**

OneTime Auth Type: **Cookies**

Session Module Type: **Disable**

Debug: **On**

RADIUS: [Shared]

- 1. Enable: On
- 2. Primary Host/Address: 192.168.100.11
- 3. Primary Secret Word: (defined)
- 4. Secondary Host/Address: (undefined)
- 5. Secondary Secret Word: (undefined)
- 6. Fallback Timer: 20 Sec
- 7. Fallback Local: On (All failures)
- 8. Retries: 3
- 9. Authentication Port: 1812
- 10. Accounting Port: 1813
- 11. Default User Access: Off
- 12. OneTime Auth: On
- 13. OneTime Auth Timer: 5
- 14. OneTime Auth Type: Cookies
- 15. Session Module Type: Disable
- 16. Debug: On
- 17. Ping Test

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