

## CISCO SYSTEMS - CX ENTERPRISE NETWORKING



# How to configure User External Authentication using TACACS?

Prepared for: Cisco DNA Customers, CX Support Teams

Prepared by: Tomas de Leon, Technical Leader

February 16, 2019

Document number: 02162019\_v1

---

**CISCO SYSTEMS - CX ENTERPRISE NETWORKING**

# TECHNOTE OF THE DAY (TOTD) -- HOW TO CONFIGURE EXTERNAL AUTHENTICATION FOR USERS USING TACACS ON THE CISCO DNAC?

## Objective

The objective of this document is to provide users an example of enabling external authentication for access to the Cisco DNAC. This technote will focus on configuring the Cisco DNAC & the Cisco ISE for using the TACACS protocol for user authentication. For this technote, there is an assumption that the integration between the Cisco DNAC and the Cisco ISE is already configured and in an "Active" state.

## Goals

Provide an example of configuring the Cisco DNAC & the Cisco ISE for using the TACACS protocol for external authentication of users.

The following technote is written against the **Cisco DNA Center version 1.2.8 Patch Release** and the **Cisco ISE version 2.4.0.357 Patch 5**. The following technote is written to help answer the questions in regards to configuring the Cisco DNAC & the Cisco ISE for using the TACACS protocol for user authentication.

## Reference Information:

- Cisco DNAC version 1.2.8
- Cisco ISE version 2.4.0.357 Patch 5

## Cisco Digital Network Architecture Center Administrator Guide, Release 1.2.8

*Chapter: Manage Users*

[https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-8/admin/b\\_dnac\\_admin\\_guide\\_1\\_2\\_8/b\\_dnac\\_admin\\_guide\\_1\\_2\\_8\\_chapter\\_0101.html](https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-8/admin/b_dnac_admin_guide_1_2_8/b_dnac_admin_guide_1_2_8_chapter_0101.html)

## TASK\_1 - VERIFY THE CISCO DNAC & CISCO ISE INTEGRATION IS CONFIGURED AND ACTIVE.

From the Cisco DNAC CUI, Goto -> **System Settings-> Settings-> Authentication and Policy Servers:**

- **Verify TACACS protocol is configured and the ISE status is "ACTIVE". If TACACS protocol is not configured, you will need to configure and enable before proceeding.**

CISCO SYSTEMS - CX ENTERPRISE NETWORKING

Settings | Data Platform | Users | Backup & Restore

### Authentication and Policy Servers

Use this page to specify the servers that authenticate DNA Center users. ISE servers can also supply policy and user information.

Last updated: 7:40 pm Refresh Export Add

Edit Delete

**\* Verify TACACS protocol is selected and the ISE status is "ACTIVE"**

IP Address	Protocol	Type	Status
172.18.217.120	RADIUS_TACACS	ISE	ACTIVE

CISCO DNA CENTER | DESIGN | POLICY | PROVISION | ASSURANCE | PLATFORM

System 360 | Software Updates | Settings | Data Platform | Users | Backup & Restore

### Authentication and Policy Servers

Use this page to specify the servers that authenticate DNA Center users.

Edit Delete

IP Address	Protocol
172.18.217.120	RADIUS_TACACS

#### Add AAA/ISE server

Server IP Address\*  
172.18.217.120

Shared Secret\*  
....

Cisco ISE server

Username\*  
admin

Password\*  
....

FQDN\*  
dna1-ise.cisco.com

Subscriber Name\*  
dna1-dnac

SSH Key

Virtual IP Address(es) ⓘ

Hide Advanced Settings

Protocol ⓘ

RADIUS  TACACS

Authentication Port\*

**\* You will need to verify that the ISE & Cisco DNAC configuration are using the SAME "Shared Secret".**

**\* Make sure that the TACACS protocol is enabled for the ISE & Cisco DNAC integration.**

## TASK\_2 - CONFIGURE CISCO ISE FOR TACACS AUTHORIZATION & AUTHENTICATION FOR THE CISCO DNAC.

- **Step 1: Enable Device Admin Service**

Administration → System → Deployment , "Enable Device Admin Service" as shown in below snapshot:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is Administration > System > Deployment > Deployment Nodes List > dna1-ise. The 'Edit Node' page is displayed, with the 'General Settings' tab selected. The node configuration includes:

- Hostname: dna1-ise
- FQDN: dna1-ise.cisco.com
- IP Address: 172.18.217.120
- Node Type: Identity Services Engine (ISE)

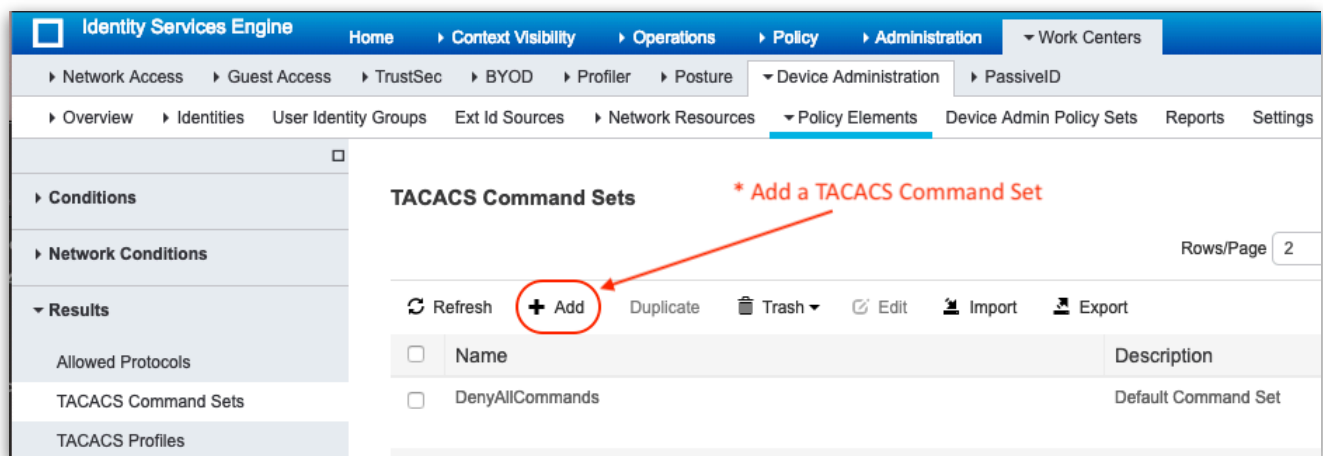
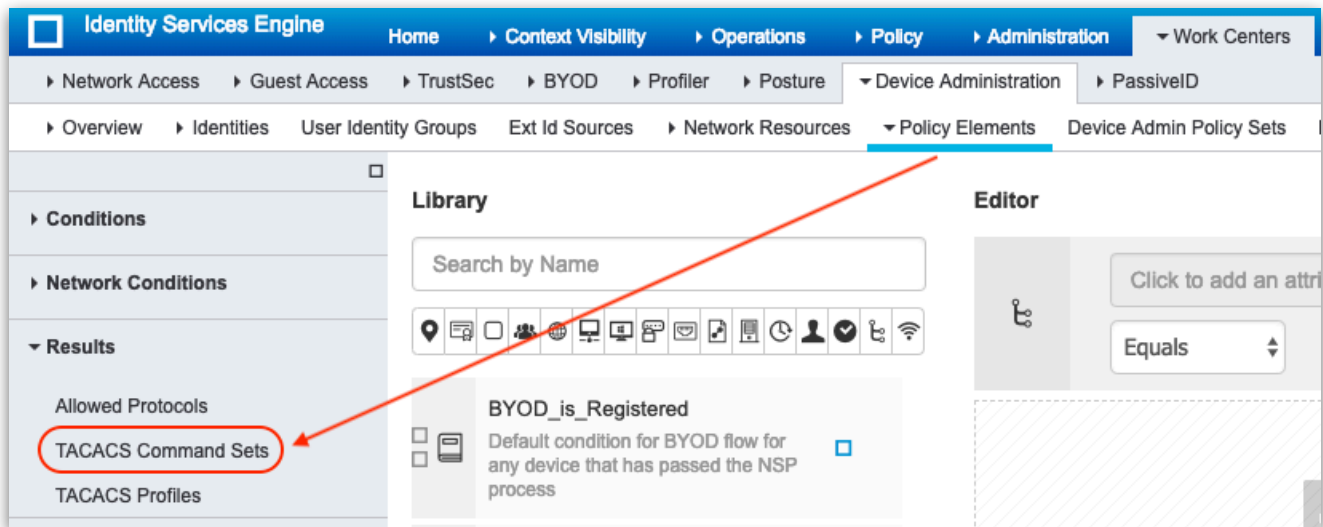
The 'Role' is set to 'STANDALONE' with a 'Make Primary' button. The following services are enabled:

- Administration
- Monitoring (Role: PRIMARY)
- Policy Service
  - Enable Session Services (Include Node in Node Group: None)
  - Enable Profiling Service
  - Enable Threat Centric NAC Service
  - Enable SXP Service (Use Interface: GigabitEthernet 1)
  - Enable Device Admin Service** (highlighted with a red circle and arrow)
  - Enable Passive Identity Service
- pxGrid

Buttons for 'Save' and 'Reset' are visible at the bottom of the configuration area.

- **Step 2: Configure TACACS Command Sets**

Under **Work Centers** → **Device Administration** → **Policy Elements** → **Results** → **TACACS Command Sets** → **add** the command set and select **"Permit any command that is not listed below"** option.



- Step 2: Configure TACACS Command Sets (cont.)

The screenshot shows the Identity Services Engine interface. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > PassiveID > Policy Elements. The page title is "TACACS Command Sets > PermitAllCommands".

**Command Set**

Name: PermitAllCommands  
 Description: Permit All Command Set

**Commands**

Permit any command that is not listed below  \* Check "Permit any command..." and SAVE

Buttons: + Add, Trash, Edit, Move Up, Move Down

<input type="checkbox"/>	Grant	Command	Arguments
No data found.			

The screenshot shows the Identity Services Engine interface. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > PassiveID > Policy Elements. The page title is "TACACS Command Sets".

Rows/Page: 2

Buttons: Refresh, + Add, Duplicate, Trash, Edit, Import, Export

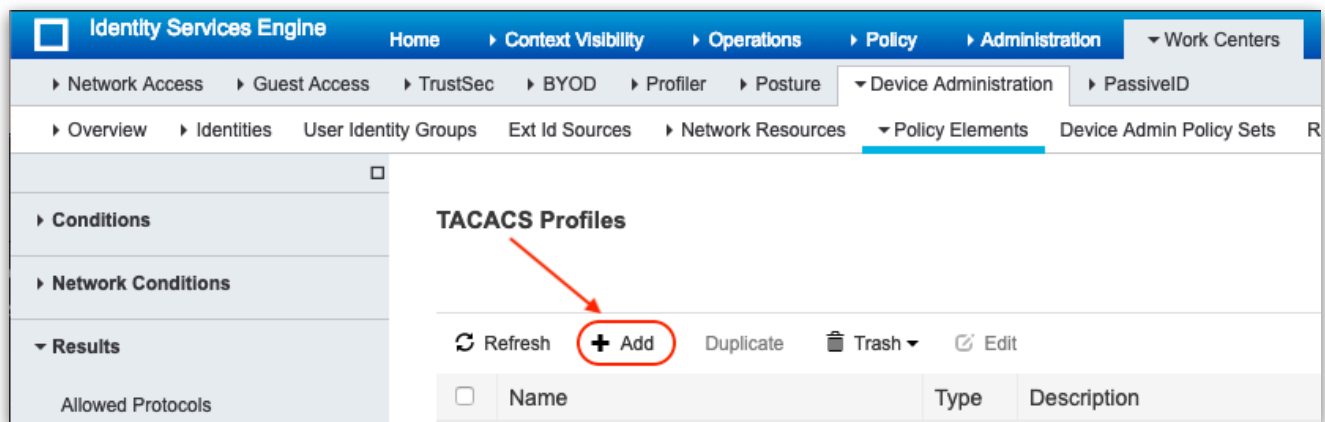
<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	DenyAllCommands	Default Command Set
<input type="checkbox"/>	PermitAllCommands	Permit All Command Set

- **Step 3: Configure TACACS Profiles**

Under **Work Centers** → **Device Administration** → **Policy Elements** add details as mentioned below & mention "**cisco-av-pair**" or "**Cisco-AVPair**" with required Role value.

The value provided here for "Role" will be validated against the Roles that exist in the Cisco DNAC, hence the values specified here should be valid roles.

**NOTE:** The Custom Attribute is what is "sent" to the Cisco DNAC. The "**Syntax**" of the cisco av pair that is configured here depends on what the Cisco DNAC is expecting. **Please refer to the Cisco DNAC configuration for the "AAA Attribute" section for more details.**



The screenshot displays the Identity Services Engine (ISE) web interface. The breadcrumb navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The main content area is titled "TACACS Profiles". Below the title, there are action buttons: Refresh, Add (circled in red with a red arrow pointing to it), Duplicate, Trash, and Edit. Below the buttons is a table with columns for Name, Type, and Description.

Name	Type	Description
------	------	-------------



**TACACS Profile**

Name: DNAC\_NETWORK\_ADMIN\_TACACS

Description: Users with DNAC NETWORK-ADMIN-ROLE Privileges

Common Task Type: Shell

- Default Privilege: 15 (Select 0 to 15)
- Maximum Privilege: (Select 0 to 15)
- Access Control List: (Select 0 to 15)
- Auto Command: (Select true or false)
- No Escape: (Select true or false)
- Timeout: (Minutes (0-9999))
- Idle Time: (Minutes (0-9999))

**Custom Attributes**

\* The Custom Attribute is what is "sent" to the Cisco DNAC. The "Syntax" of the cisco av pair that is configured here depends on what the Cisco DNAC is expecting. Please refer to the Cisco DNAC configuration for the "AAA Attribute" section for more details.

Type	Name	Value
<input type="checkbox"/> MANDATORY	Cisco-AVPair	Role=NETWORK-ADMIN-ROLE

Buttons: Cancel, Save

**TACACS Profiles**

\* You can add different TACACS profiles for different User Roles

Rows/Page: 8

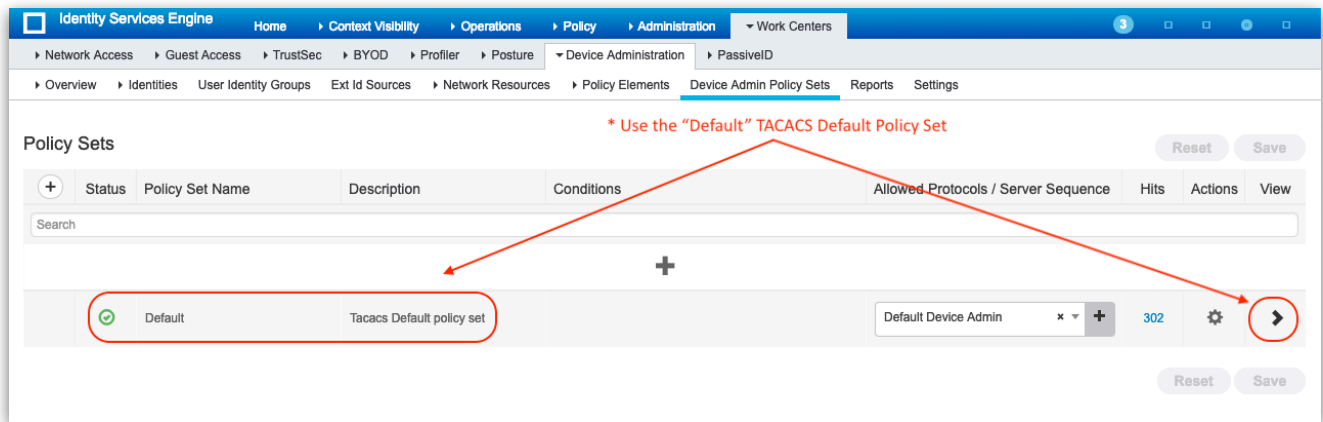
Refresh Add Duplicate Trash Edit

Name	Type	Description
<input type="checkbox"/> DNAC_NETWORK_ADMIN_TACACS	Shell	Users with DNAC NETWORK-ADMIN-ROLE Privileges
<input type="checkbox"/> DNAC_OBSERVER_TACACS	Shell	Users with DNAC OBSERVER-ROLE Privileges
<input type="checkbox"/> DNAC_SUPER_ADMIN_TACACS	Shell	Users with DNAC SUPER-ADMIN-ROLE Privileges
<input type="checkbox"/> DNAC_TELEMETRY_ADMIN_TACACS	Shell	Users with TELEMETRY-ADMIN-ROLE Privileges
<input type="checkbox"/> Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/> Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/> WLC ALL	WLC	WLC ALL
<input type="checkbox"/> WLC MONITOR	WLC	WLC MONITOR



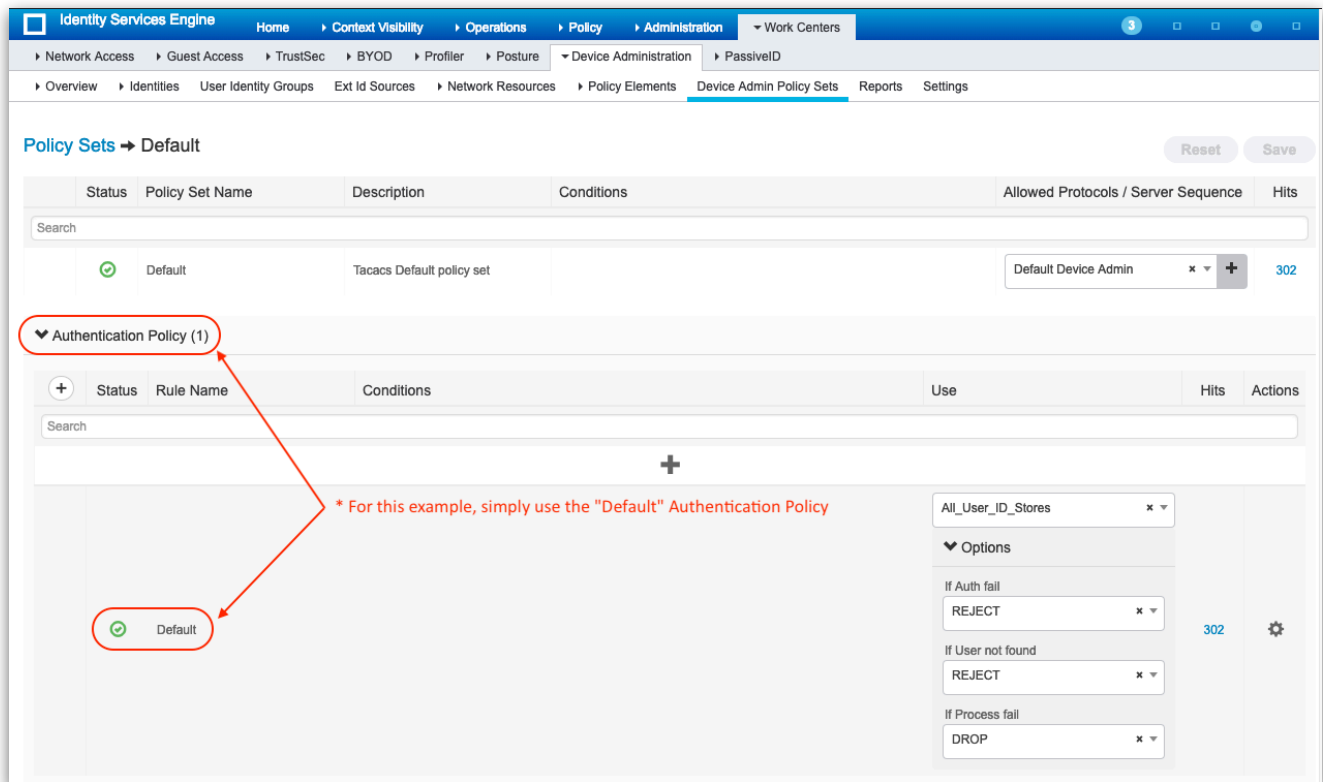
- **Step 4: Configure Authentication & Authorization Policies for TACACS**

Under **Work Center** → **Device Administration** → **Device Admin Policy Set** → **Default** →



### "Authentication Policy"

For this example, simply use the "**Default**" Authentication Policy



### "Authorization Policy"

& create required Authorization Rules & mention the Shell profile created in previous steps.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	
✔	Default	Tacacs Default policy set		Default Device Admin	302	
➤ Authentication Policy (1)						
➤ Authorization Policy - Local Exceptions						
➤ Authorization Policy - Global Exceptions						
▼ Authorization Policy (5)						
+	Status	Rule Name	Conditions	Results	Hits	Actions
	✔	DNAC-TELEMETRY-ADMIN-ROLE	IdentityGroup-Name EQUALS User Identity Groups:DNAC-TELEMETRY-ADMIN-ROLE	PermitAllCommands	0	⚙
	✔	DNAC-OBSERVER-ROLE	IdentityGroup-Name EQUALS User Identity Groups:DNAC-OBSERVER-ROLE	PermitAllCommands	8	⚙
	✔	DNAC-NETWORK-ADMIN-ROLE	IdentityGroup-Name EQUALS User Identity Groups:DNAC-NETWORK-ADMIN-ROLE	PermitAllCommands	26	⚙
	✔	DNAC-SUPER-ADMIN-ROLE	IdentityGroup-Name EQUALS User Identity Groups:DNAC-SUPER-ADMIN-ROLE	PermitAllCommands	156	⚙
	✔	Default		DenyAllCommands	0	⚙

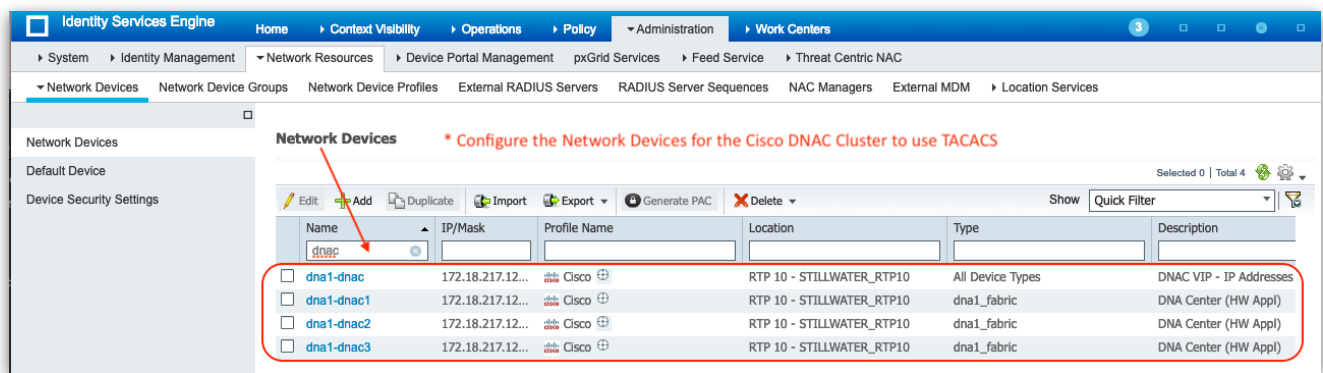
As part of condition, associate to users. These **users** will be created as shown in **step 6**.

✔	DNAC-OBSERVER-ROLE	IdentityGroup-Name EQUALS User Identity Groups:DNAC-OBSERVER-ROLE	PermitAllCommands	DNAC_OBSERVER_TACACS	8	⚙
✔	DNAC-NETWORK-ADMIN-ROLE	IdentityGroup-Name EQUALS User Identity Groups:DNAC-NETWORK-ADMIN-ROLE	PermitAllCommands	DNAC_NETWORK_ADMIN_...	26	⚙
✔	DNAC-SUPER-ADMIN-ROLE	IdentityGroup-Name EQUALS User Identity Groups:DNAC-SUPER-ADMIN-ROLE	PermitAllCommands	DNAC_SUPER_ADMIN_TA...	156	⚙
✔	Default		DenyAllCommands	Deny All Shell Profile	0	⚙

• **Step 5: Configure the Network Devices for the Cisco DNAC Cluster to use TACACS**

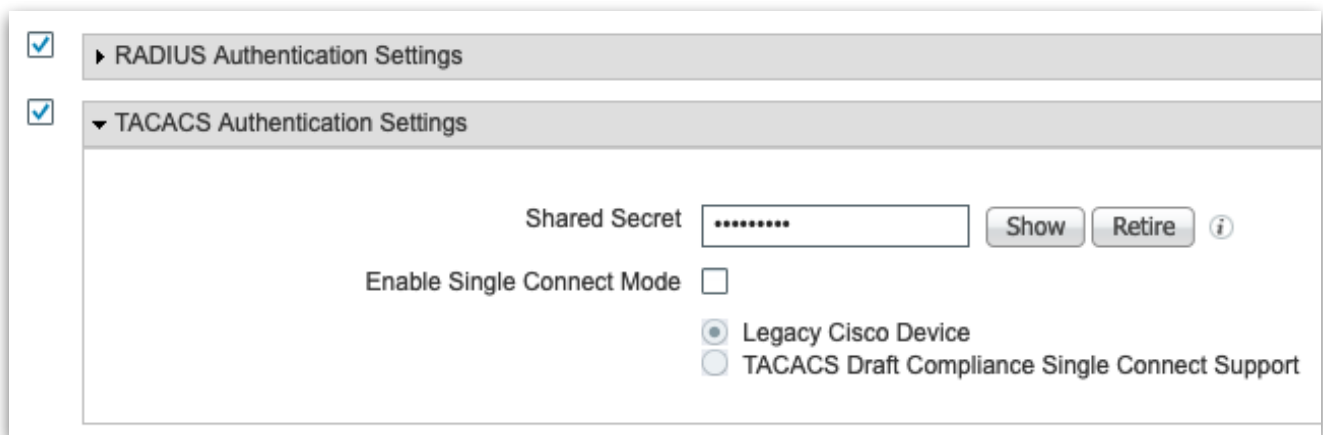
Under **Administration** → **Network Resources** → **Network Devices**, select the defined Cisco DNAC Device entries.

**Note:** *If a Network Device is not present, Add a Network Device for "each" Cisco DNAC in the Cluster. In addition, Add a Network Device for the Virtual IPs (VIPs).*



Under **Administration** → **Network Devices**, select **"Enable TACACS"** and configure the Shared Secret value - which will be used while configuring the ISE on DNAC Common Settings page.

If specific device/IP address entries are present in "Network Devices" tab, enable TACACs settings there as well.



**Identity Services Engine** Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Network Devices > Network Device Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > External MDM > Location Services

Network Devices List > dna1-dnac

### Network Devices

\* Name:

Description:

IP Address	* IP	Mask	Actions
<input type="text" value="172.18.217.129"/>	<input type="text" value="172.18.217.129"/>	<input type="text" value="32"/>	
<input type="text" value="10.0.0.124"/>	<input type="text" value="10.0.0.124"/>	<input type="text" value="32"/>	
<input type="text" value="192.68.211.124"/>	<input type="text" value="192.68.211.124"/>	<input type="text" value="32"/>	
<input type="text" value="172.18.242.129"/>	<input type="text" value="172.18.242.129"/>	<input type="text" value="32"/>	

\* Device Profile:

Model Name:

Software Version:

\* Network Device Group

Location:

IPSEC:

Device Type:

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret:

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

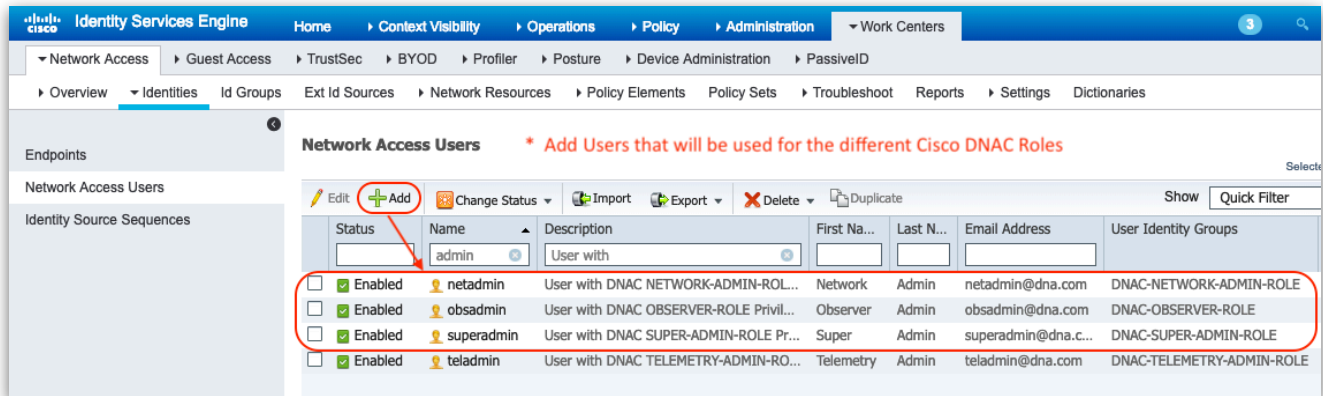
SNMP Settings

Advanced TrustSec Settings

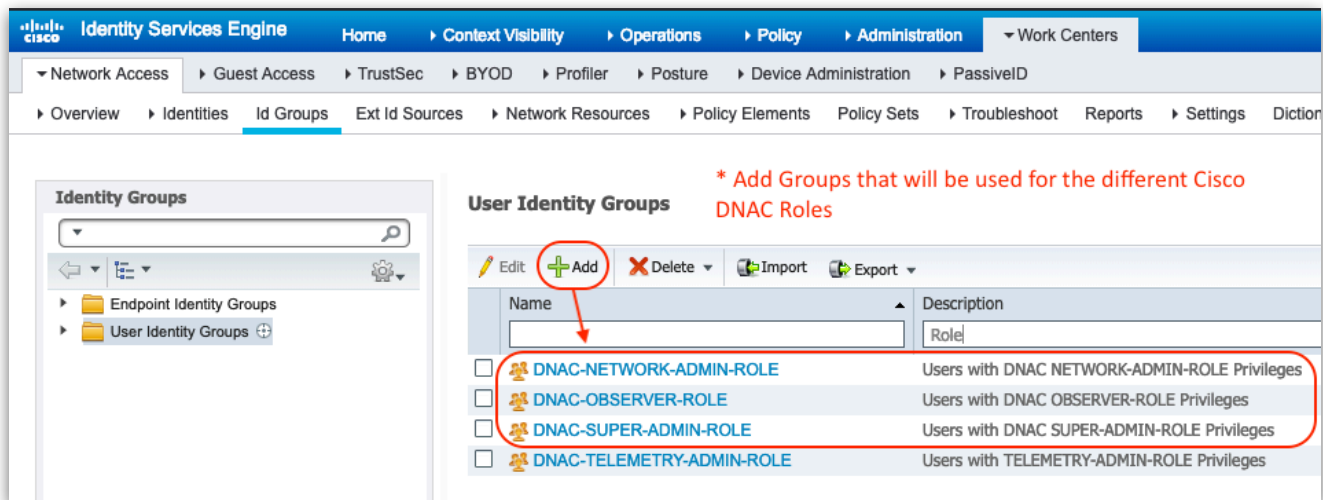
*\* Select "Enable TACACS" and configure the Shared Secret value - which will be used while configuring the ISE on DNAC Common Settings page.*

- **Step 6: Add Users & Groups that will be used for the different Cisco DNAC Roles**

Under **Work Center** → **Network Access** → **Identities** → **Network Access Users** → **click Add** & mention the details as shown below :



Under **Work Center** → **Network Access** → **Id Groups** → **User Identity Groups** → **click Add** & mention the details as shown below :



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Id Groups. The left sidebar shows a tree view with 'Endpoint Identity Groups' and 'User Identity Groups'. The main content area is titled 'User Identity Groups > DNAC-NETWORK-ADMIN-ROLE'. It displays the configuration for an Identity Group with the name 'DNAC-NETWORK-ADMIN-ROLE' and description 'Users with DNAC NETWORK-ADMIN-ROLE Privileges'. Below this, there are 'Save' and 'Reset' buttons. A red warning message states: '\* Add the Cisco DNAC Users for each defined Role'. Underneath, there is a table of 'Member Users' with columns for Status, Email, Username, First Name, and Last Name. The table contains three entries, all with 'Enabled' status.

**Identity Groups**

Search: [ ]

- Endpoint Identity Groups
- User Identity Groups

User Identity Groups > **DNAC-NETWORK-ADMIN-ROLE**

**Identity Group**

\* Name:

Description:

**Member Users** \* Add the Cisco DNAC Users for each defined Role

Users Selected 0 | Total 3

Show:

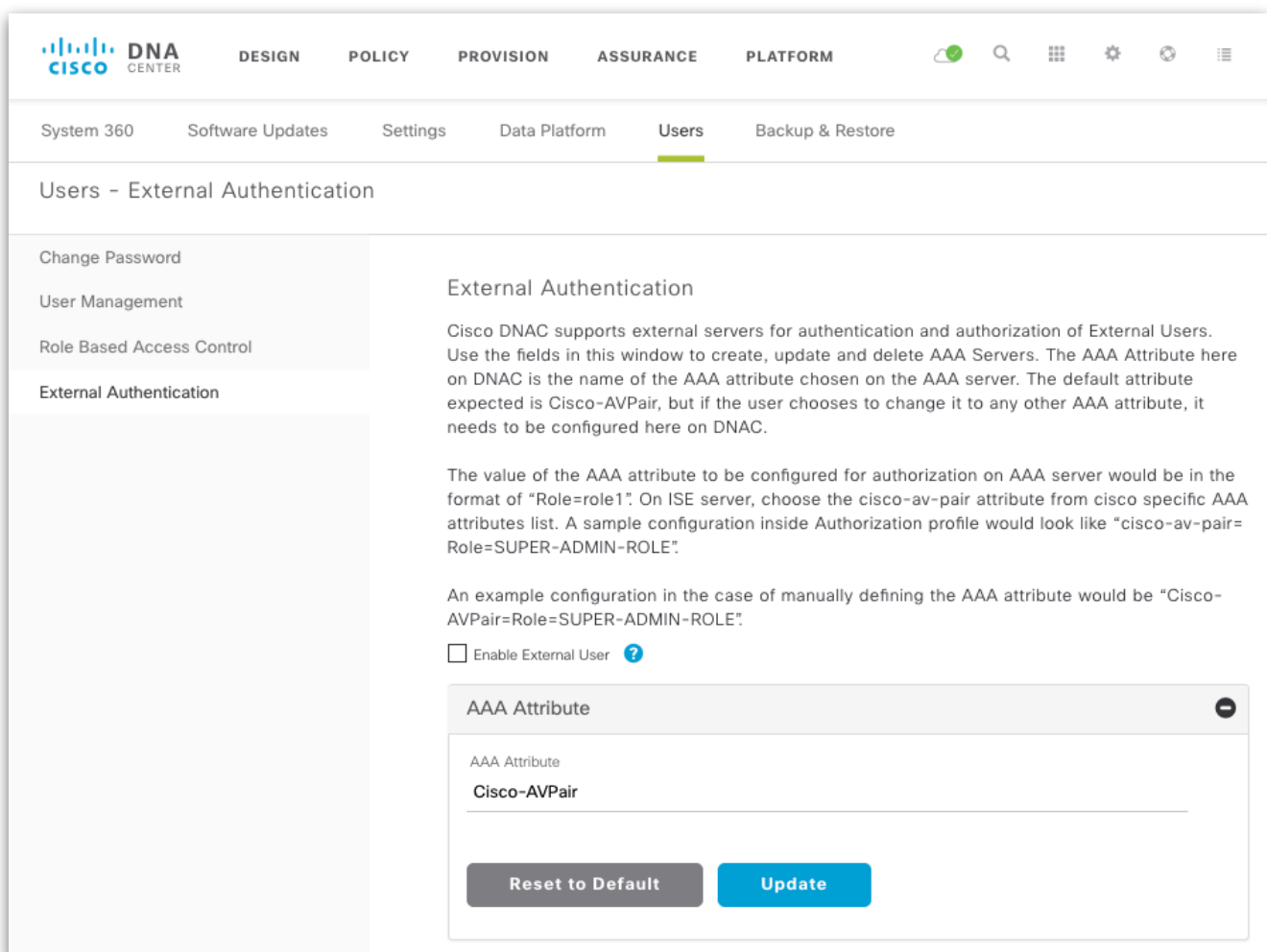
Status	Email	Username	First Name	Last Name
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled	tacadmin@DNA.com	tacadmin	TAC	ADMIN
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled	deadbeef@DNA.com	deadbeef	Ponce	de Leon
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled	netadmin@dna.com	netadmin	Network	Admin

### TASK\_3 - CONFIGURE CISCO DNAC USER MANAGEMENT FOR EXTERNAL AUTHENTICATION USING TACACS.

From the Cisco DNAC GUI, Goto -> **System Settings-> Users-> External Authentication**

This task is important to pay attention to each step that you perform when enabling external authentication. **The AAA Attribute value for "cisco av pair" can change based on an action that you perform.** The AAA Attribute value that you configured in TASK\_2 needs to match what the Cisco DNAC is expecting for the authentication credentials exchange.

The **default** attribute expected for Cisco-AVPair is **"cisco-av-pair"**.



The screenshot displays the Cisco DNAC Center interface. The top navigation bar includes 'DESIGN', 'POLICY', 'PROVISION', 'ASSURANCE', and 'PLATFORM'. Below this, a secondary menu shows 'System 360', 'Software Updates', 'Settings', 'Data Platform', 'Users', and 'Backup & Restore'. The 'Users' section is active, leading to 'Users - External Authentication'.

The left sidebar contains options: 'Change Password', 'User Management', 'Role Based Access Control', and 'External Authentication' (which is highlighted).

The main content area is titled 'External Authentication' and contains the following text:

Cisco DNAC supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and delete AAA Servers. The AAA Attribute here on DNAC is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user chooses to change it to any other AAA attribute, it needs to be configured here on DNAC.

The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role1". On ISE server, choose the cisco-av-pair attribute from cisco specific AAA attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair=Role=ADMIN-ROLE".

An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=ADMIN-ROLE".

Enable External User [?](#)

**AAA Attribute**

AAA Attribute  
Cisco-AVPair

Reset to Default Update



- **Step 1: Enable External User Authentication**

To Enable External User simply **CHECK "Enable External User"**. **Do Not Press "UPDATE" Button**. The Cisco DNAC will notify configuration with the message **"Success: Successfully saved external authentication settings."**

The screenshot shows the Cisco DNA Center interface for configuring external authentication. The left sidebar contains navigation options: Change Password, User Management, Role Based Access Control, and External Authentication. The main content area is titled 'External Authentication' and includes explanatory text about AAA attributes and servers. A red circle highlights the 'Enable External User' checkbox, which is checked. A red arrow points from this checkbox to a 'Success' notification box in the bottom right corner. The notification box contains a green checkmark and the text 'Success: Successfully saved external authentication settings.'

**\* To Enable External User simply CHECK "Enable External User". Do Not Press "UPDATE" Button.**

If you checked "Enable External User" and Do Not Press "UPDATE" Button, the following is the syntax used when configuring the ISE TACACS Profile. This is the "Original" DEFAULT AAA Attribute value.

**cisco-av-pair**                    **ROLE=NETWORK-ADMIN-ROLE**

<input type="checkbox"/>	Type	Name	Value
<input type="checkbox"/>	MANDATORY	cisco-av-pair	ROLE=NETWORK-ADMIN-ROLE

**Gotcha\_1:** If you checked "Enable External User" and then Pressed "UPDATE" Button, the following is the syntax used when configuring the ISE TACACS Profile. This is the "New" DEFAULT AAA Attribute value.

**Cisco-AVPair**                    **Role=NETWORK-ADMIN-ROLE**

<input type="checkbox"/>	Type	Name	Value
<input type="checkbox"/>	MANDATORY	Cisco-AVPair	Role=NETWORK-ADMIN-ROLE

**Option\_2:** If you checked "Enable External User", Changed the AAA Attribute, and then Pressed "UPDATE" Button, the following is the syntax used when configuring the ISE TACACS Profile. For this example. "custom-av-pair" is the AAA Attribute value.

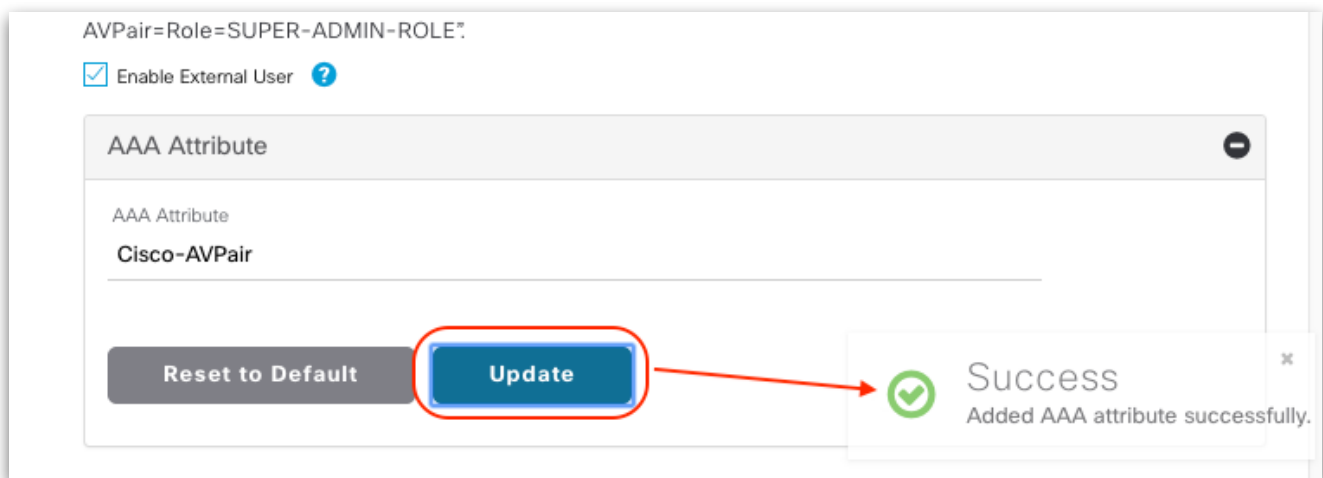
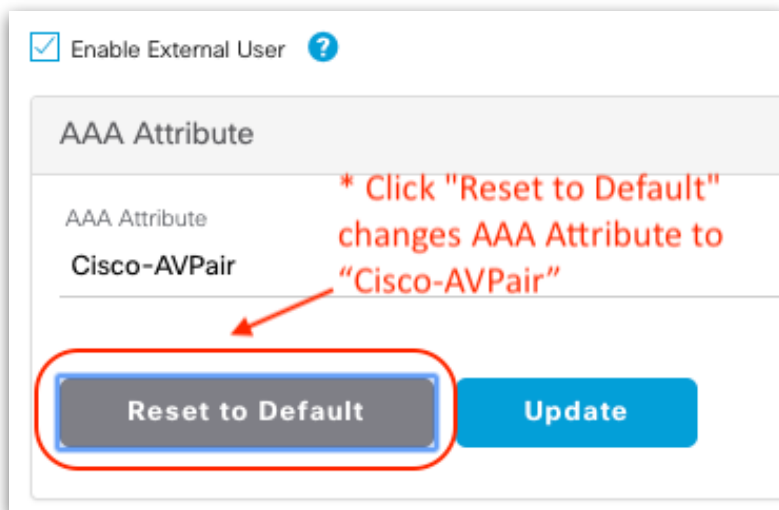
**custom-av-pair**                    **Role=NETWORK-ADMIN-ROLE**

The screenshot shows a configuration window for 'Enable External User'. At the top, there is a checked checkbox labeled 'Enable External User' with a help icon. Below this is a section titled 'AAA Attribute'. Inside this section, the text 'AAA Attribute' is followed by 'custom-av-pair'. Below the text are two buttons: a grey 'Reset to Default' button and a blue 'Update' button. A red circle highlights the 'Update' button, and a red arrow points from the 'custom-av-pair' text to the 'Update' button.

<input type="checkbox"/>	Type	Name	Value
<input type="checkbox"/>	MANDATORY	custom-av-pair	Role=NETWORK-ADMIN-ROLE

**Gotcha 2:** If you changed the AAA Attribute to and you want to **reset** the AAA Attribute **BACK TO THE DEFAULT** value, perform the following:

- Click "**Reset to Default**"
- Click "**Update**"



The gotcha is that the "New" **DEFAULT** AAA Attribute value is "**Cisco-AVPair**" **not** the original DEFAULT of "cisco-av-pair". So in ISE, configure:

**Cisco-AVPair Role=NETWORK-ADMIN-ROLE**

<input type="checkbox"/>	Type	Name	Value
<input type="checkbox"/>	MANDATORY	Cisco-AVPair	Role=NETWORK-ADMIN-ROLE

- **Step 2: Select AAA Server(s) to be used for External Authentication using TACACS**

✓ Under the AAA Server(s) section, select the ISE Server.

**Note:** If the server(s) is not listed in the dropdown, try refreshing the browser to re-list available servers.

✓ Select TACACS Protocol.

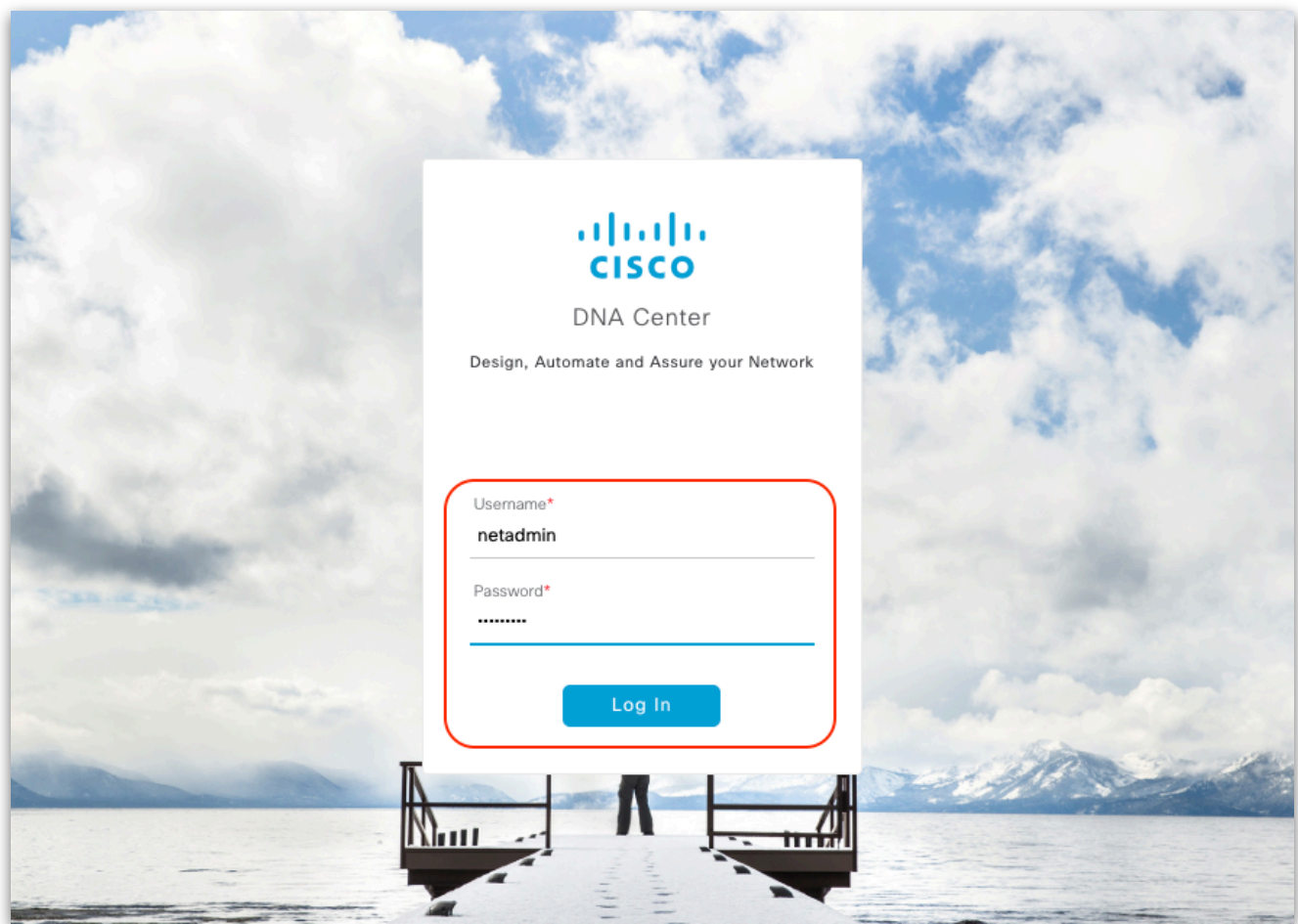
**Note:** The TACACS protocol port number is 49. This is not configurable in Cisco DNAC version 1.2.8 or later.

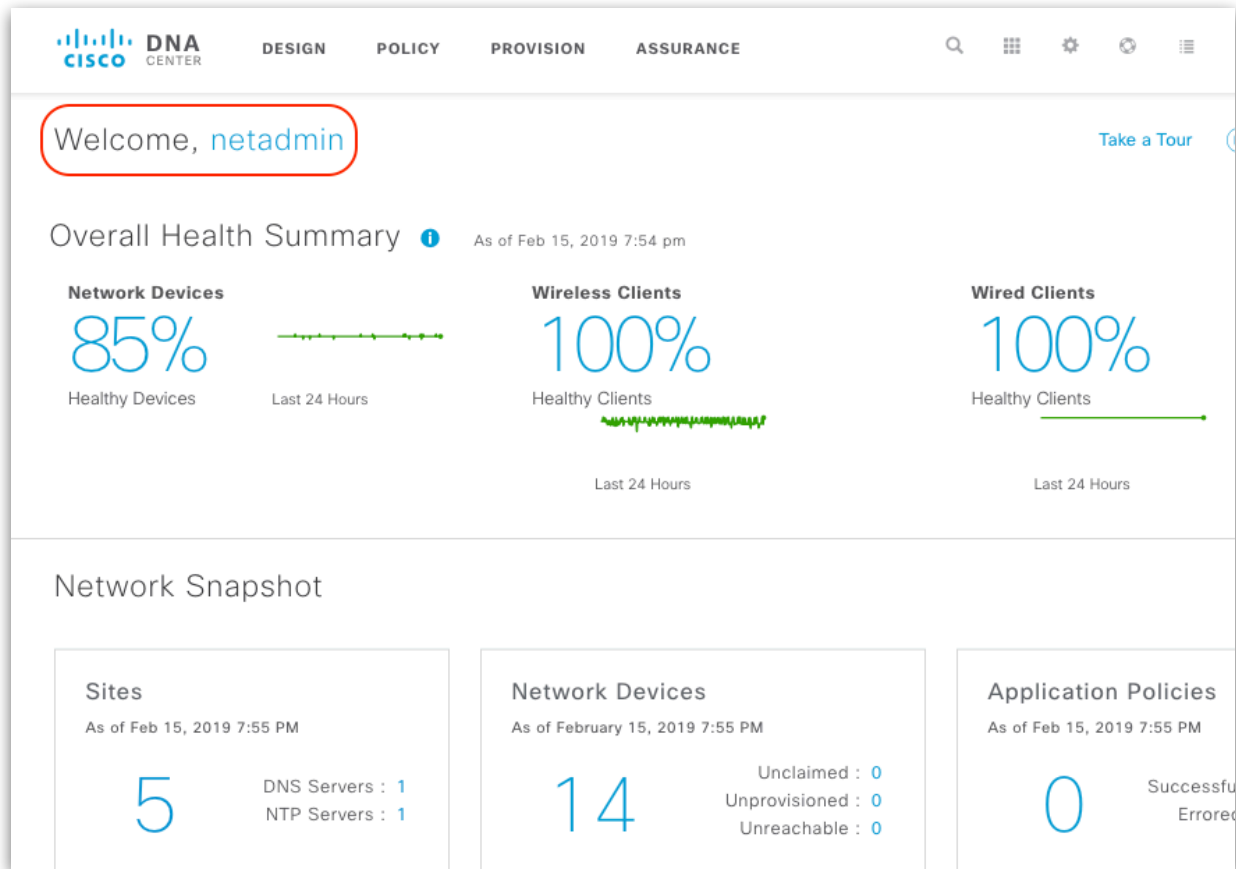
✓ Click UPDATE to save changes

The screenshot shows the configuration page for an AAA Attribute and its associated AAA Server(s). At the top, there is a checkbox for "Enable External User" which is checked. Below this, the "AAA Attribute" section shows "Cisco-AVPair" as the selected attribute, with "Reset to Default" and "Update" buttons. The "AAA Server(s)" section shows a "Primary AAA Server" with an IP address of "172.18.217.120". Underneath, there is a "Shared Secret" field with an eye icon. A "Hide Advanced Settings" link is present. The "Protocol" section has two radio buttons: "RADIUS" (unselected) and "TACACS" (selected). Below the protocol, the "Port" is set to "49", "Retries" is "1", and "Timeout (seconds)" is "2". At the bottom right, there is an "Update" button. Red circles and arrows highlight the "TACACS" radio button, the "49" port value, and the "Update" button.

#### TASK\_4 - VERIFY CISCO DNAC USER MANAGEMENT FOR EXTERNAL AUTHENTICATION USING TACACS WITH CISCO ISE.

- Sign out of the Cisco DNAC GUI
- Login into the Cisco DNAC GUI using one of the Users that you configured earlier.



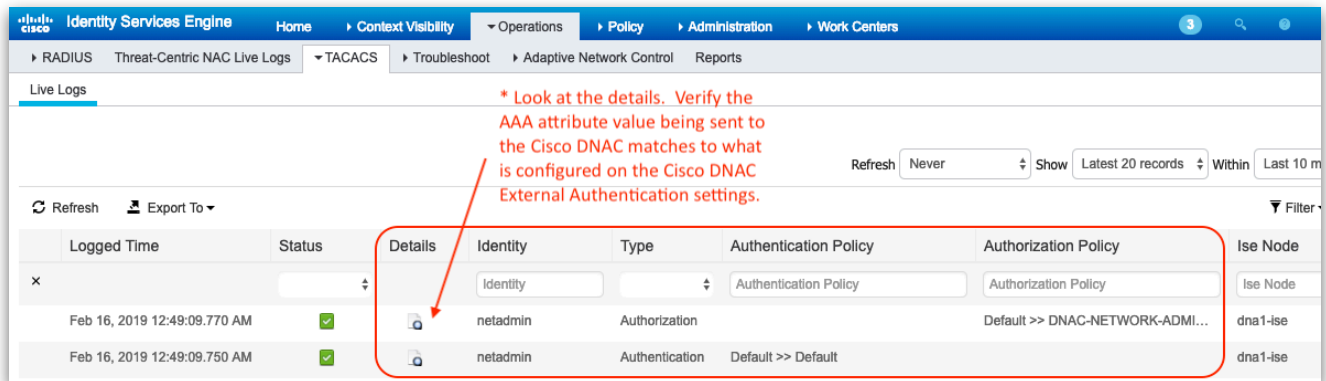
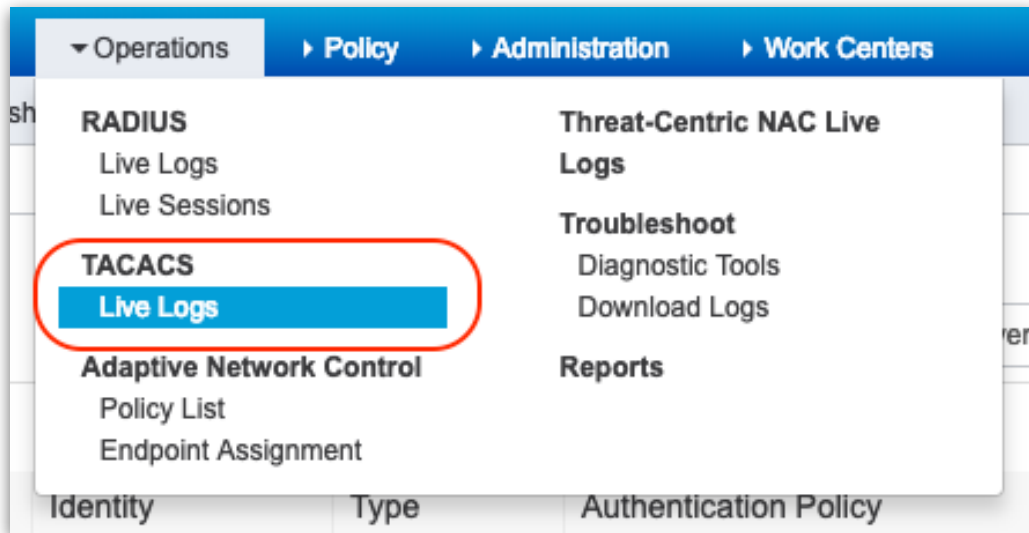


- From the Cisco DNAC GUI, Goto -> **System Settings-> Users-> External Authentication**  
**Look at the External Users list.** You should see the TACACS users listed and their assigned roles.

External Users	
Username	Role
bdeaver	OBSERVER-ROLE
ciscotac	OBSERVER-ROLE
cssuser	OBSERVER-ROLE
deadbeef	NETWORK-ADMIN-ROLE
netadmin	NETWORK-ADMIN-ROLE
obsadmin	OBSERVER-ROLE

**APPENDIX - TROUBLESHOOTING.**

On the ISE, Start your troubleshooting by looking at the **TACACS Live Logs**. Verify the ISE is sending the correct "cisco av pair" to the Cisco DNAC Cluster.





### Steps

- 13005 Received TACACS+ Authorization Request
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15041 Evaluating Identity Policy
- 22072 Selected identity source sequence - All\_User\_ID\_Stores
- 15013 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore
- 24212 Found User in Internal Users IDStore
- 22037 Authentication Passed
- 15036 Evaluating Authorization Policy
- 15048 Queried PIP - Network Access.UserName
- 15048 Queried PIP - IdentityGroup.Name
- 15017 Selected Shell Profile
- 22081 Max sessions policy passed
- 22080 New accounting session created in Session cache
- 13034 Returned TACACS+ Authorization Reply

### Authorization Attributes

All Request Attributes

All Response Attributes

Cisco-AVPair=Role=NETWORK-ADMIN-ROLE,priv-lvl=15

### TACACS Protocol

Authentication Method	TacacsPlus
Authentication Privilege Level	0
Authentication Type	PAP
Authentication Service	Login

**Overview**

Request Type	Authorization
Status	Pass
Session Key	dna1-ise/333167629/783820
Message Text	Device-Administration: Session Authorization succeeded
Username	netadmin
Authorization Policy	Default >> DNAC-NETWORK-ADMIN-ROLE
Shell Profile	DNAC_NETWORK_ADMIN_TACACS
Matched Command Set	
Command From Device	

**Authorization Details**

Generated Time	2019-02-16 00:49:09.77 +0:00
Logged Time	2019-02-16 00:49:09.77
Epoch Time (sec)	1550278149
ISE Node	dna1-ise
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	netadmin
Network Device Name	dna1-dnac3
Network Device IP	172.18.217.123
Network Device Groups	Device Type#All Device Types#dna1_fabric,IPSEC#Is IPSEC Device#No,Location#All Locations#RTP 10 - STILLWATER_RTP10
Device Type	Device Type#All Device Types#dna1_fabric
Location	Location#All Locations#RTP 10 - STILLWATER_RTP10
Device Port	console
Remote Address	localhost

**Other Attributes**

ConfigVersionId	384
DestinationIPAddress	172.18.217.120
DestinationPort	49
UserName	netadmin
Protocol	Tacacs
RequestLatency	10
Type	Authorization
Service-Argument	cas-service
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
IdentityGroup	User Identity Groups:DNAC-NETWORK-ADMIN-ROLE
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_AD_Join_Points
SelectedAuthenticationIdentityStores	Guest Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	1451316186172.18.217.12333906Authorization1451316186
IdentitySelectionMatchedRule	Default
Network Device Profile	Cisco
IPSEC	IPSEC#is IPSEC Device#No
Name	User Identity Groups:DNAC-NETWORK-ADMIN-ROLE
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Cisco-AVPair=Role=NETWORK-ADMIN-ROLE; AVPair=priv-lvl=15; }

On the **Cisco DNAC CLI**, you can also check some logs for possible issues:

```
$ magctl appstack status | egrep "identitymgmt"  
$ magctl service logs -rf identitymgmt-1140144783-m3d12 -c identitymgmt
```

```
## User_ID that is failing is "netadmin"  
$ sudo grep -RHlrnis "netadmin" /var/log/pods
```

**For Example:**

### **FAILED - Login**

```
$ magctl appstack status | egrep "identitymgmt"  
maglev-system          identitymgmt-1140144783-107fz  
maglev-system          identitymgmt-1140144783-m3d12
```

```
$ magctl service logs -rf identitymgmt-1140144783-m3d12 -c identitymgmt
```

```
{"timeMillis":  
1550280597257,"thread":"qtp864326906-31","level":"ERROR","loggerName":"com.cisco.  
maglev.services.IdentityAccessManager","message":"Authentication has failed.  
Please provide valid  
credentials.","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg  
er","threadId":31,"threadPriority":5}
```

```
{"timeMillis":  
1550280597257,"thread":"qtp864326906-31","level":"ERROR","loggerName":"com.cisco.  
maglev.services.IdentityAccessManager","message":"Authentication has failed.  
Please provide valid  
credentials.","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg  
er","threadId":31,"threadPriority":5}
```

```
{"timeMillis":  
1550280597257,"thread":"qtp864326906-31","level":"ERROR","loggerName":"com.cisco.  
maglev.identitymgmt.api.TokenEndPoint","message":"Authentication has failed.  
Please provide valid  
credentials.","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg  
er","threadId":31,"threadPriority":5}  
$ sudo grep -RHirnis "netadmin" /var/log/pods
```

```
/var/log/pods/5bc407de-04e5-11e9-89d8-b4de31bd7aa0/cas-service_0.log:455:  
{"log":"17:57:53.242 [qtp1394438858-19298] ERROR  
com.cisco.maglev.radius.utils.CustomJRadiusServerImpl - Error while getting AAA  
Server details : User (netadmin) not authenticated.  
\n","stream":"stdout","time":"2019-01-03T17:57:53.242826244Z"}
```

```
/var/log/pods/5bc407de-04e5-11e9-89d8-b4de31bd7aa0/cas-service_0.log:455:  
{"log":"17:57:53.242
```

```
$ sudo cat ./5bc407de-04e5-11e9-89d8-b4de31bd7aa0/cas-service_0.log | egrep  
"17:57:53."
```

```
{"log":"TACACS+: Connected to server at  
172.18.217.120:49\n","stream":"stdout","time":"2019-01-03T17:57:53.128949781Z"}  
{"log":"17:57:53.210 [qtp1394438858-19298] ERROR  
com.cisco.maglev.tacacs.TacacsAuthentication -  
authenSessioncom.augur.tacacs.SessionClient@2bd3a42e\n","stream":"stdout","time":  
"2019-01-03T17:57:53.211242995Z"}  
{"log":"17:57:53.242 [qtp1394438858-19298] ERROR  
com.cisco.maglev.radius.utils.CustomJRadiusServerImpl - Error while getting AAA  
Server details : User (netadmin) not authenticated.  
\n","stream":"stdout","time":"2019-01-03T17:57:53.242826244Z"}
```

## Successful Login

```
{"timeMillis":  
1550281951650,"thread":"qtp864326906-31","level":"INFO","loggerName":"com.cisco.m  
aglev.identitymgmt.api.TokenEndPoint","message":"JWT token is generated  
successfully.","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLog  
ger","threadId":31,"threadPriority":5}
```

```
{"timeMillis":  
1550281951650,"thread":"qtp864326906-31","level":"INFO","loggerName":"com.cisco.m  
aglev.identitymgmt.api.TokenEndPoint","message":"Cookie is set  
successfully.","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLog  
ger","threadId":31,"threadPriority":5}
```

```
{"timeMillis":  
1550281951651,"thread":"qtp864326906-31","level":"INFO","loggerName":"com.cisco.m  
aglev.identitymgmt.api.TokenEndPoint","message":"'netadmin' logged in  
successfully.","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLog  
ger","threadId":31,"threadPriority":5}
```

```
{"timeMillis":  
1550281953112,"thread":"qtp864326906-32","level":"INFO","loggerName":"com.cisco.m  
aglev.sdk.persistence.document.BaseDocumentDao","message":"The number of entities  
found is  
15","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threa  
dId":32,"threadPriority":5}
```

```
timeMillis":  
1550281951651,"thread":"qtp864326906-31","level":"INFO","loggerName":"com.cisco.m  
aglev.identitymgmt.api.TokenEndPoint","message":"'netadmin' logged in  
successfully.","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLog  
ger","threadId":31,"threadPriority":5}
```

```
{"timeMillis":  
1550281953112,"thread":"qtp864326906-32","level":"INFO","loggerName":"com.cisco.m  
aglev.sdk.persistence.document.BaseDocumentDao","message":"The number of entities  
found is  
15","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threa  
dId":32,"threadPriority":5}
```