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

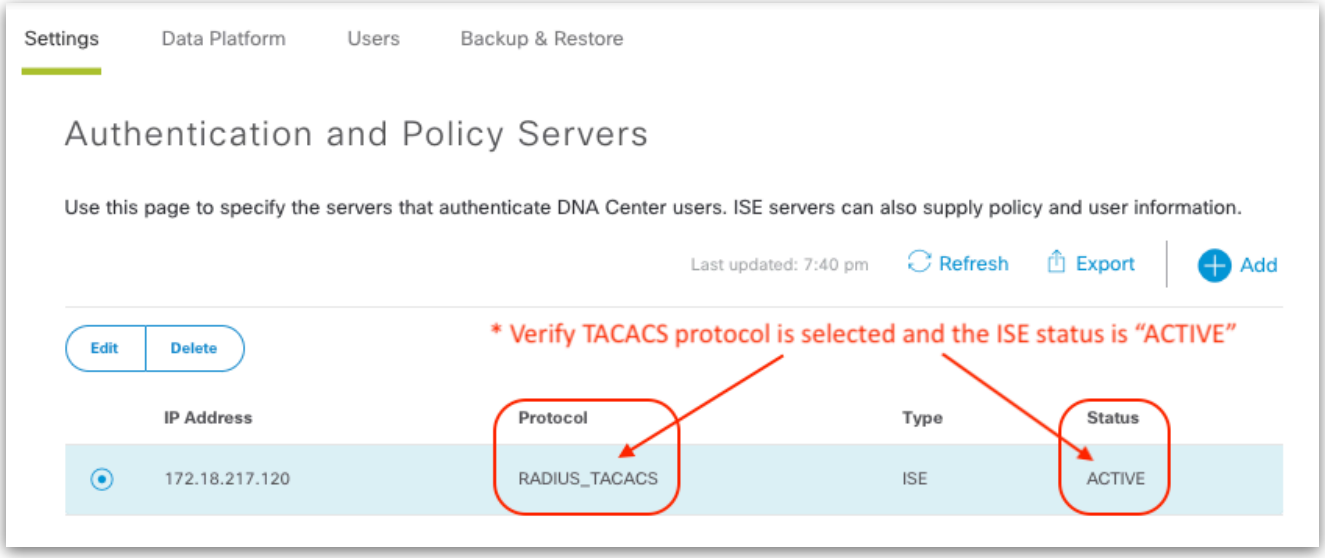
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-8/admin/b_dnac_admin_guide_1_2_8/b_dnac_admin_guide_1_2_8_chapter_0101.html

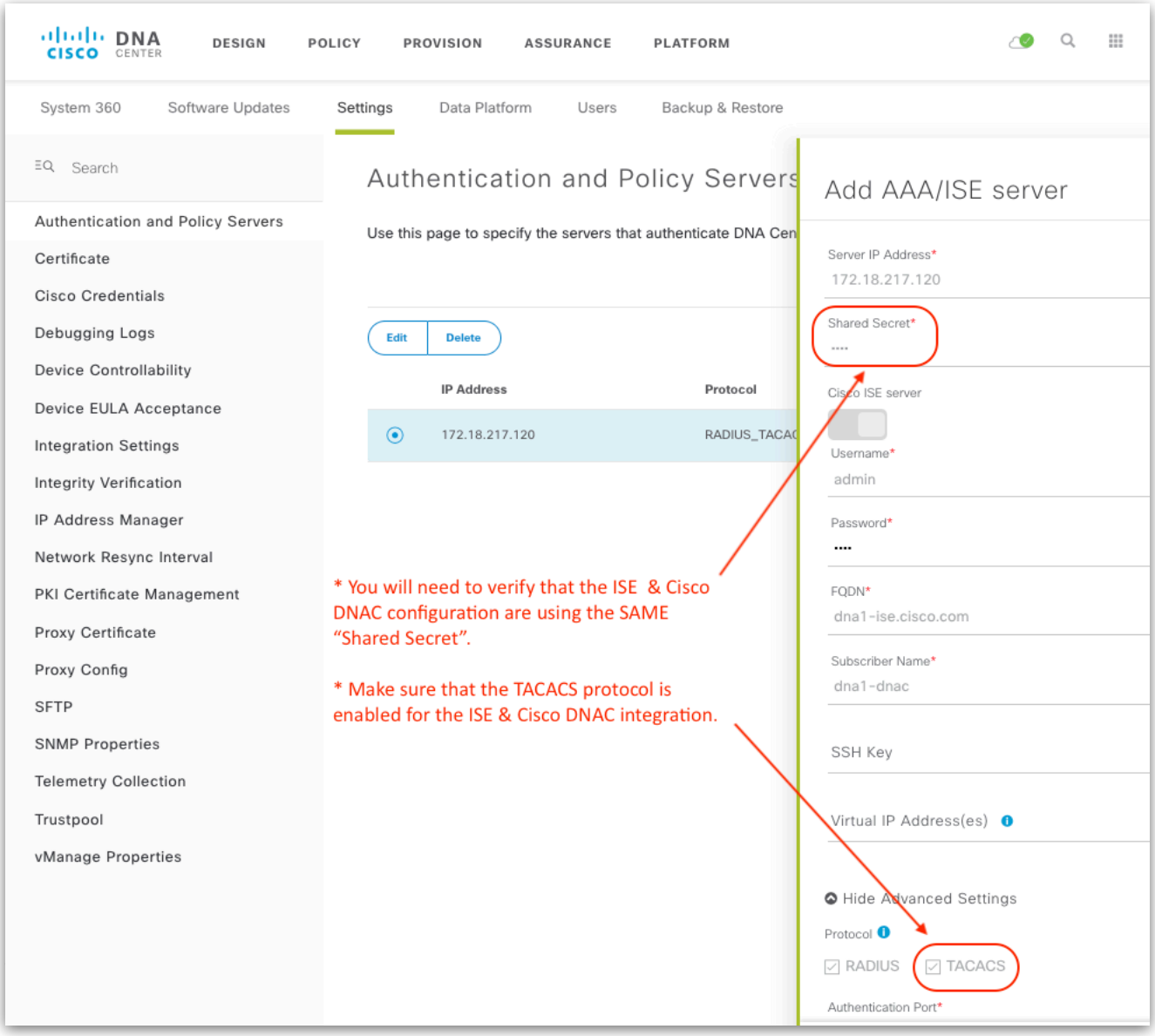
TASK_1 - VERIFY THE CISCO DNAC & CISCO ISE INTEGRATION IS CONFIGURED AND ACTIVE.

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 t configure and enable before proceeding.**

CISCO SYSTEMS - CX ENTERPRISE NETWORKING

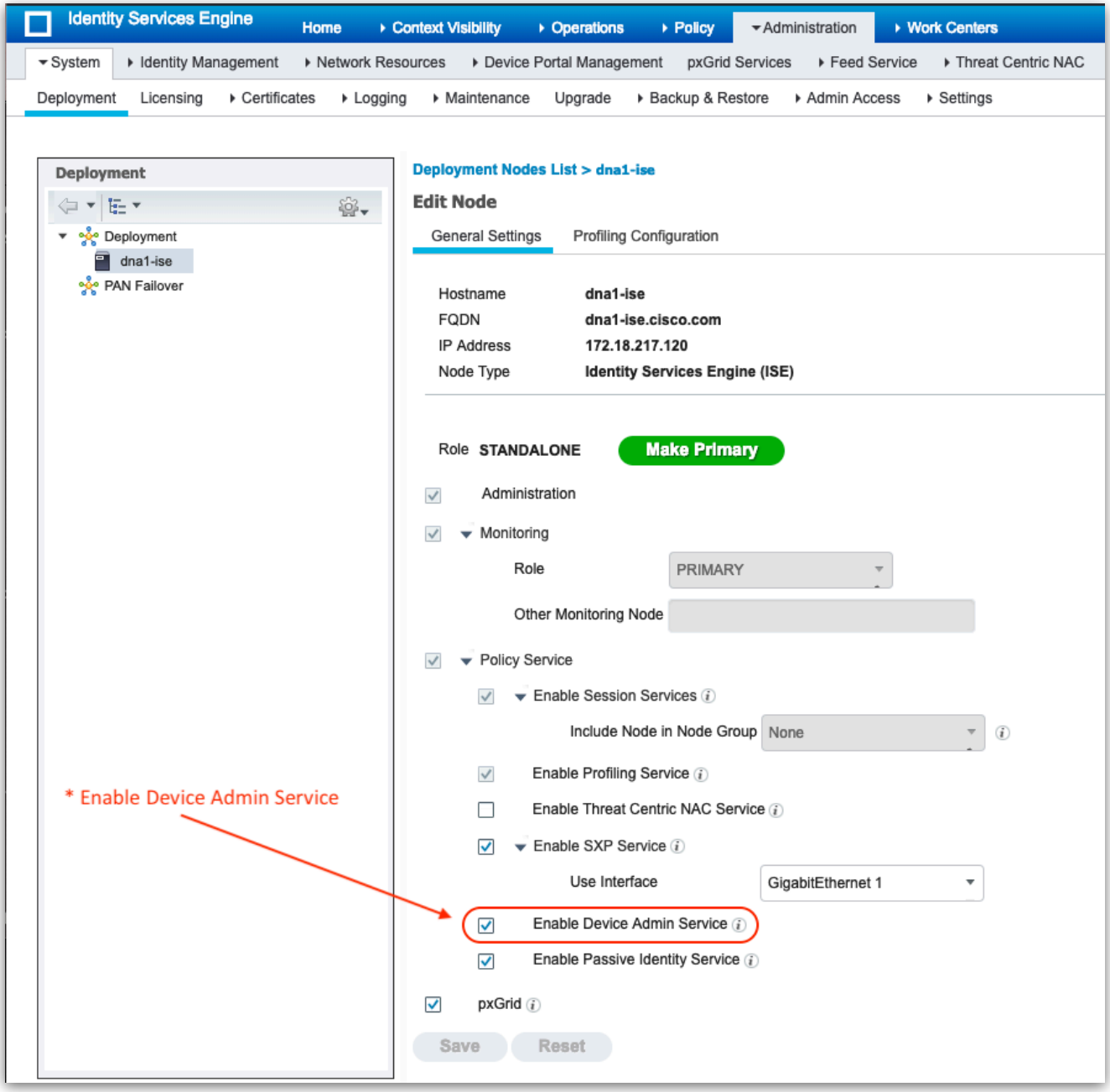




TASK_2 - CONFIGURE CISCO ISE FOR TACACS AUTHORIZATION & AUTHENTICATION FOR THE CISCO DNAC.

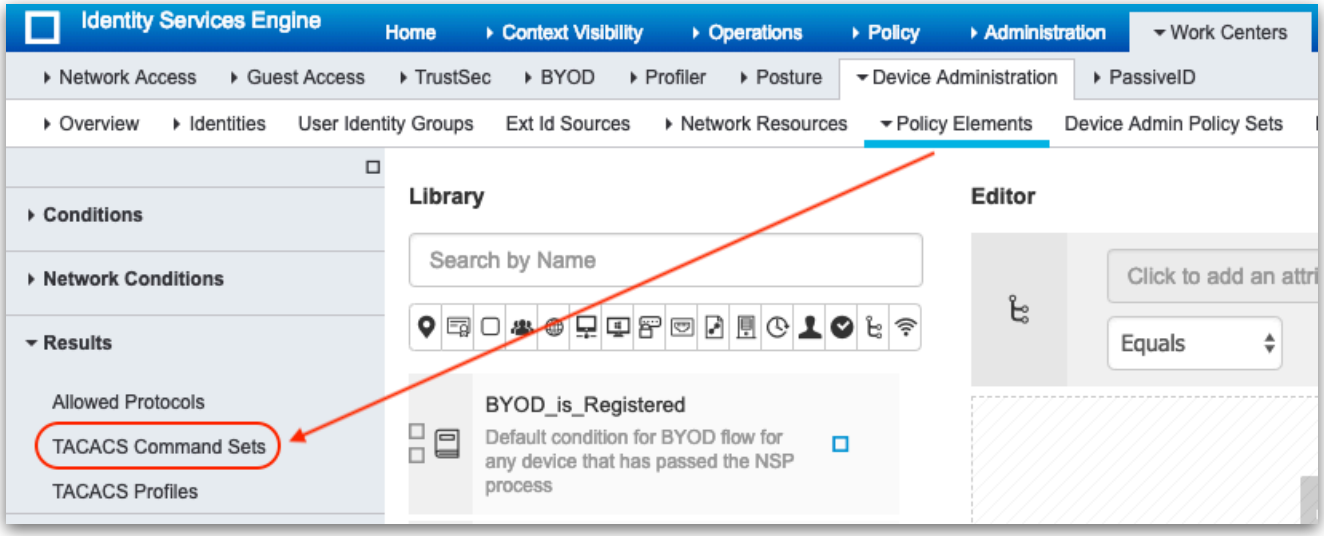
- **Step 1: Enable Device Admin Service**

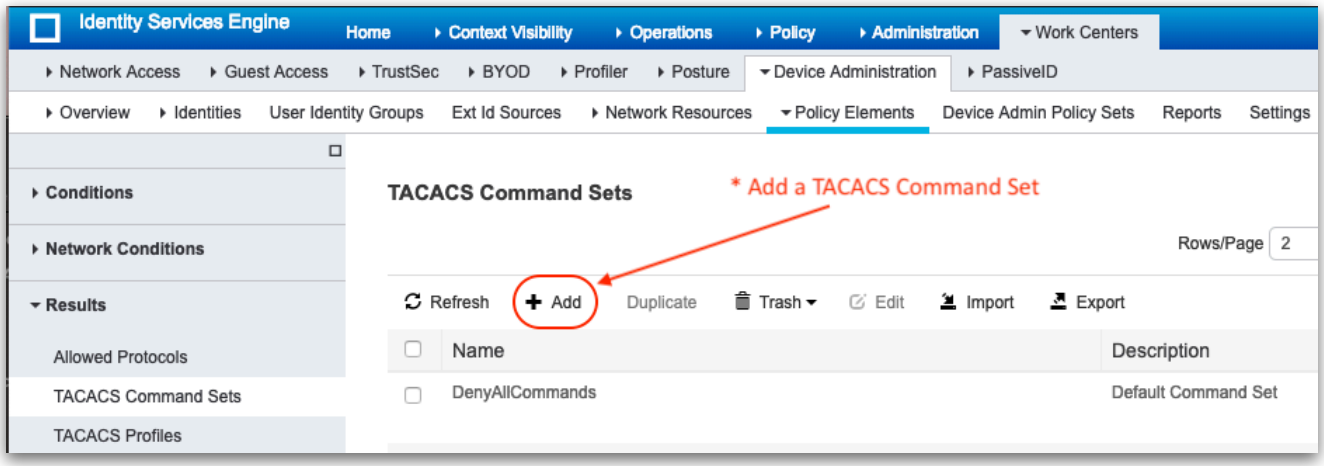
Administration → System → Deployment , "**Enable Device Admin Service**" as shown in below snapshot:



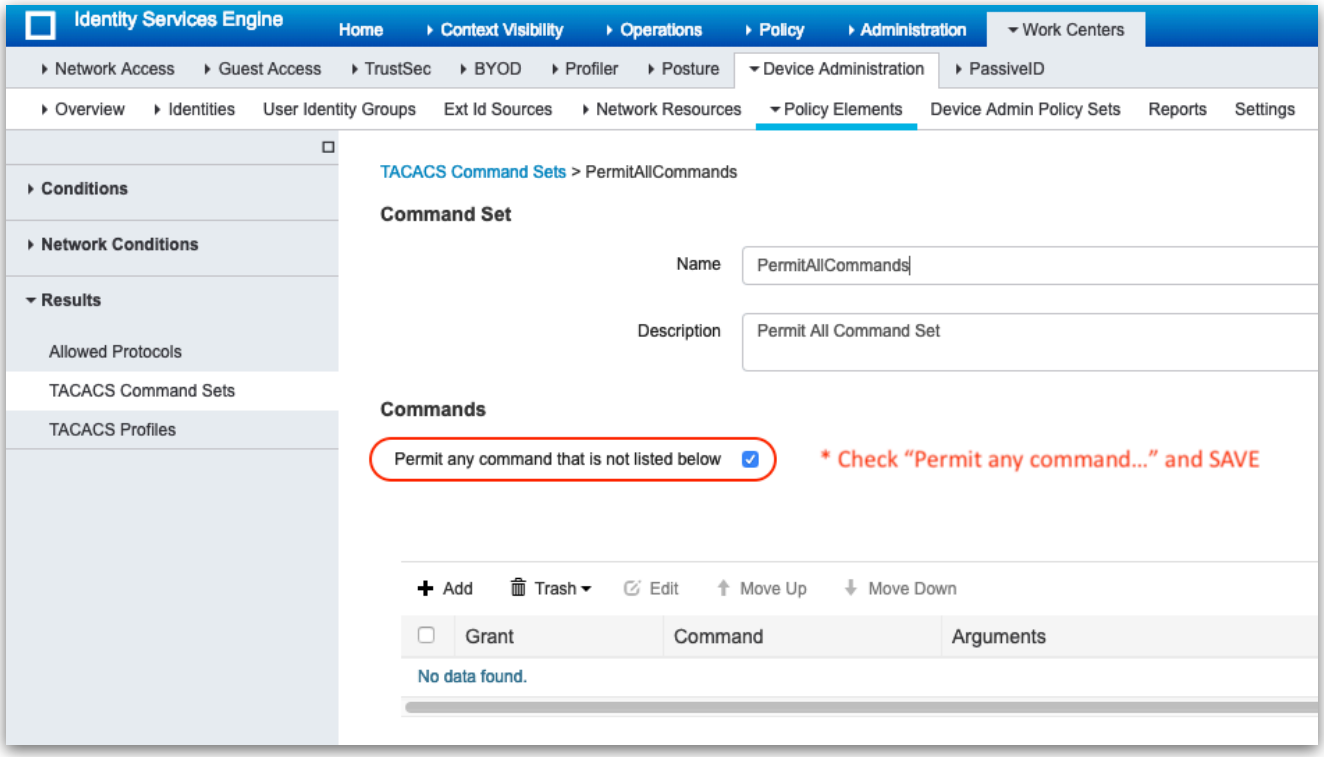
- **Step 2: Configure TACACS Command Sets**

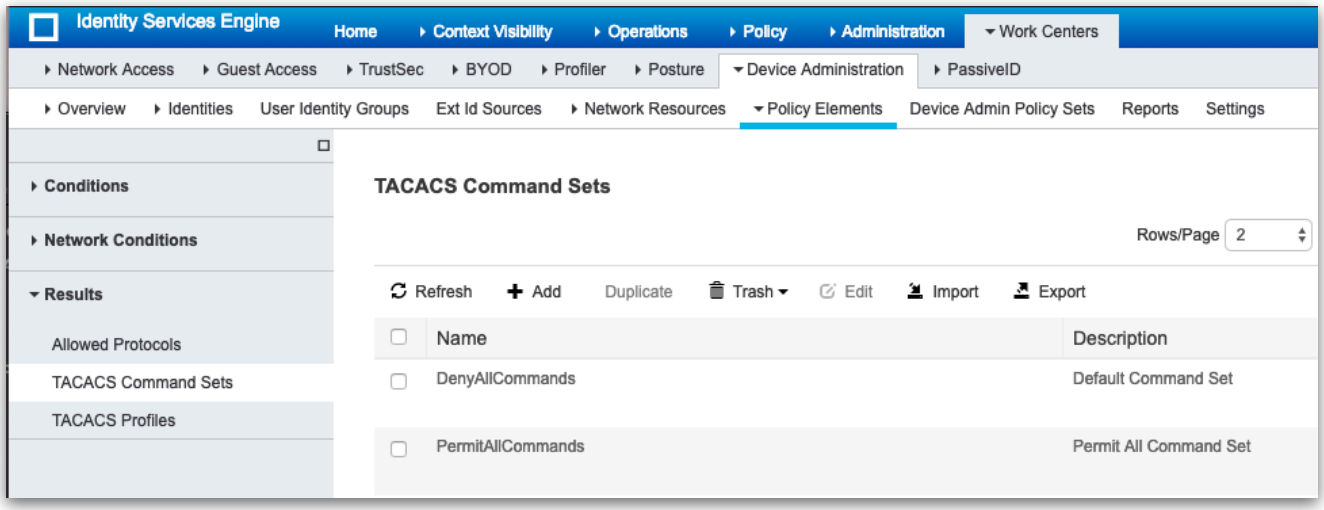
Under **Work Centers → Device Administration → Policy Elements → Results → TACACS Command Sets → add** the command set **and select "Permit any command that is not listed below"** option.





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



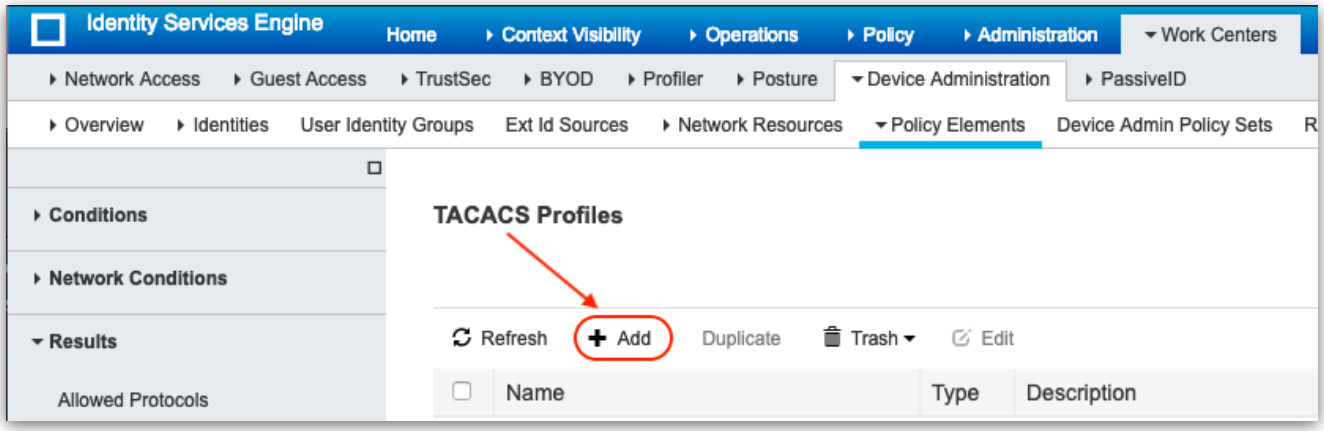


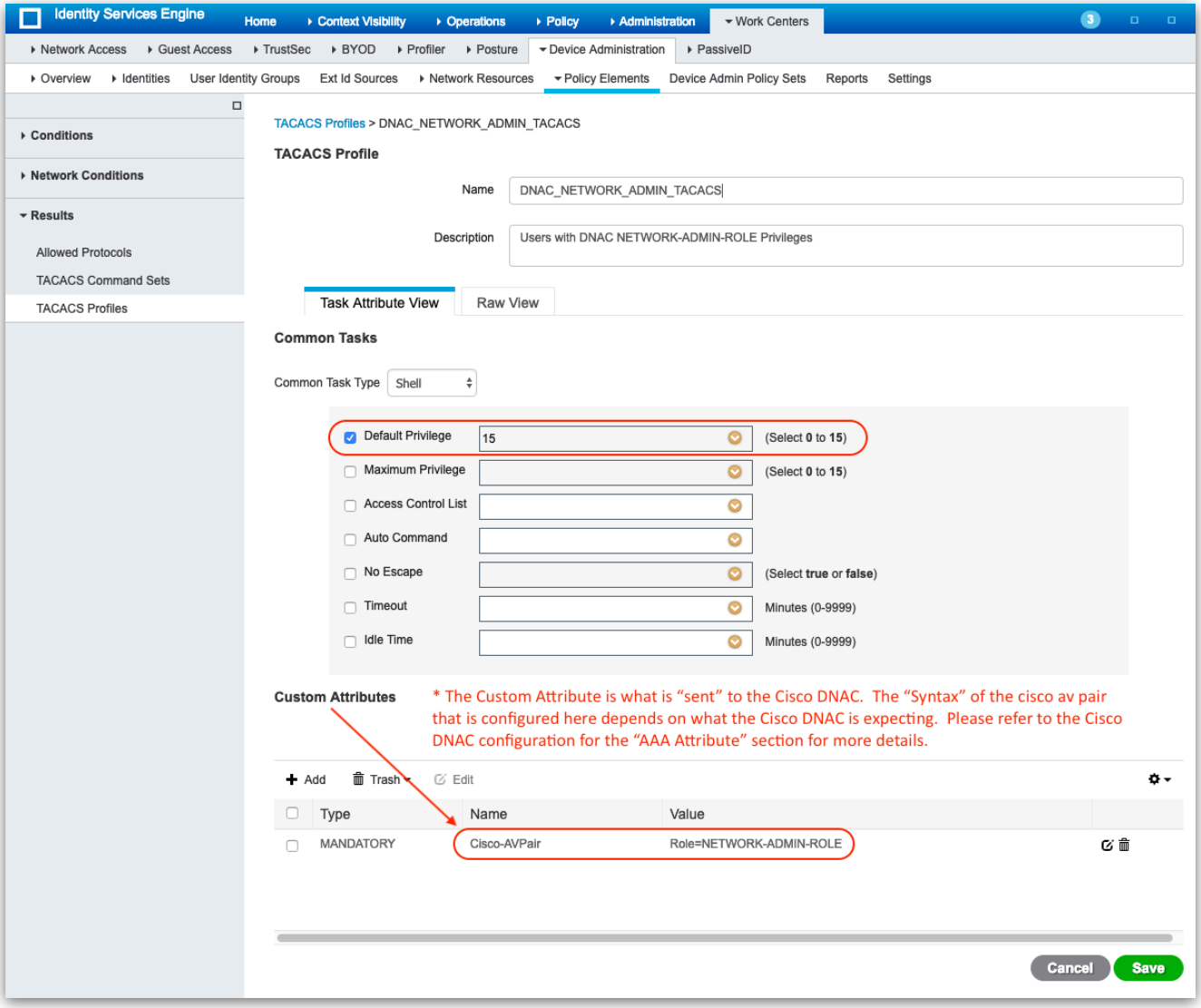
- **Step 3: Configure TACACS Profiles**

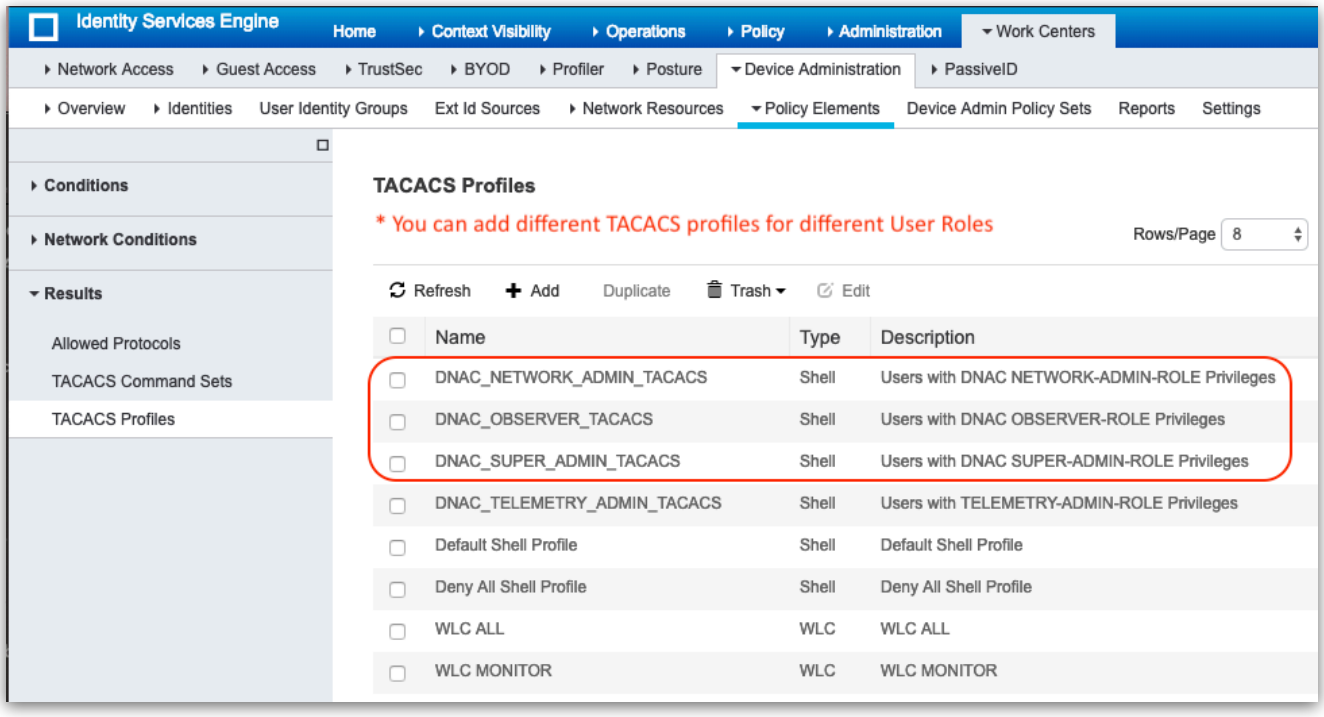
Under **Work Centers → Device Administration → Policy Elements** add details as mentioned below & mention "**cisco-av-pair**" or "**Cisco-AVPair**" with required Role value.

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.***

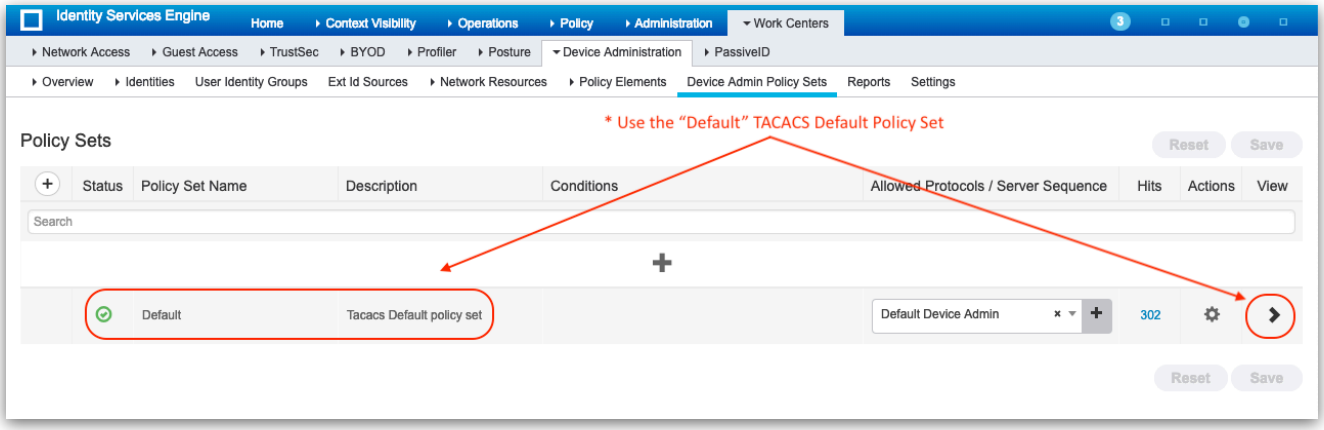



Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
Device Admin Policy Sets
Reports
Settings
Conditions
Network Conditions
Results
Allowed Protocols
TACACS Command Sets
TACACS Profiles
TACACS Profiles > DNAC_NETWORK_ADMIN_TACACS
TACACS Profile
Name
DNAC_NETWORK_ADMIN_TACACS
Description
Users with DNAC NETWORK-ADMIN-ROLE Privileges
Task Attribute View
Raw View
Common Tasks
Common Task Type
Shell
Default Privilege
15
(Select 0 to 15)
Maximum Privilege
(Select 0 to 15)
Access Control List
Auto Command
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.
Add
Trash
Edit
Type
Name
Value
MANDATORY
Cisco-AVPair
Role=NETWORK-ADMIN-ROLE
Cancel
Save


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
Device Admin Policy Sets
Reports
Settings
Conditions
Network Conditions
Results
Allowed Protocols
TACACS Command Sets
TACACS Profiles
TACACS Profiles
* You can add different TACACS profiles for different User Roles
Rows/Page
8
Refresh
Add
Duplicate
Trash
Edit
Name
Type
Description
DNAC_NETWORK_ADMIN_TACACS
Shell
Users with DNAC NETWORK-ADMIN-ROLE Privileges
DNAC_OBSERVER_TACACS
Shell
Users with DNAC OBSERVER-ROLE Privileges
DNAC_SUPER_ADMIN_TACACS
Shell
Users with DNAC SUPER-ADMIN-ROLE Privileges
DNAC_TELEMETRY_ADMIN_TACACS
Shell
Users with TELEMETRY-ADMIN-ROLE Privileges
Default Shell Profile
Shell
Default Shell Profile
Deny All Shell Profile
Shell
Deny All Shell Profile
WLC ALL
WLC
WLC ALL
WLC MONITOR
WLC
WLC MONITOR

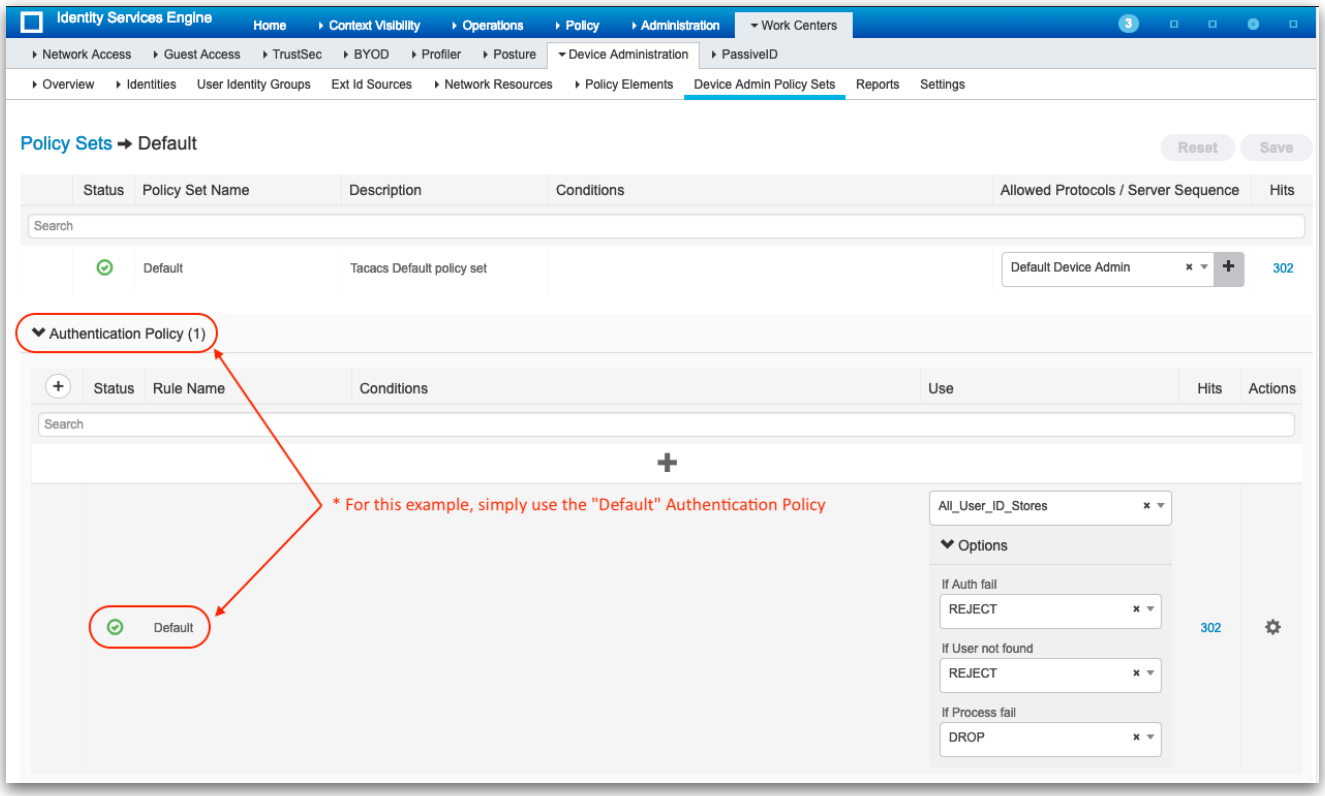
- **Step 4: Configure Authentication & Authorization Policies for TACACS**

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

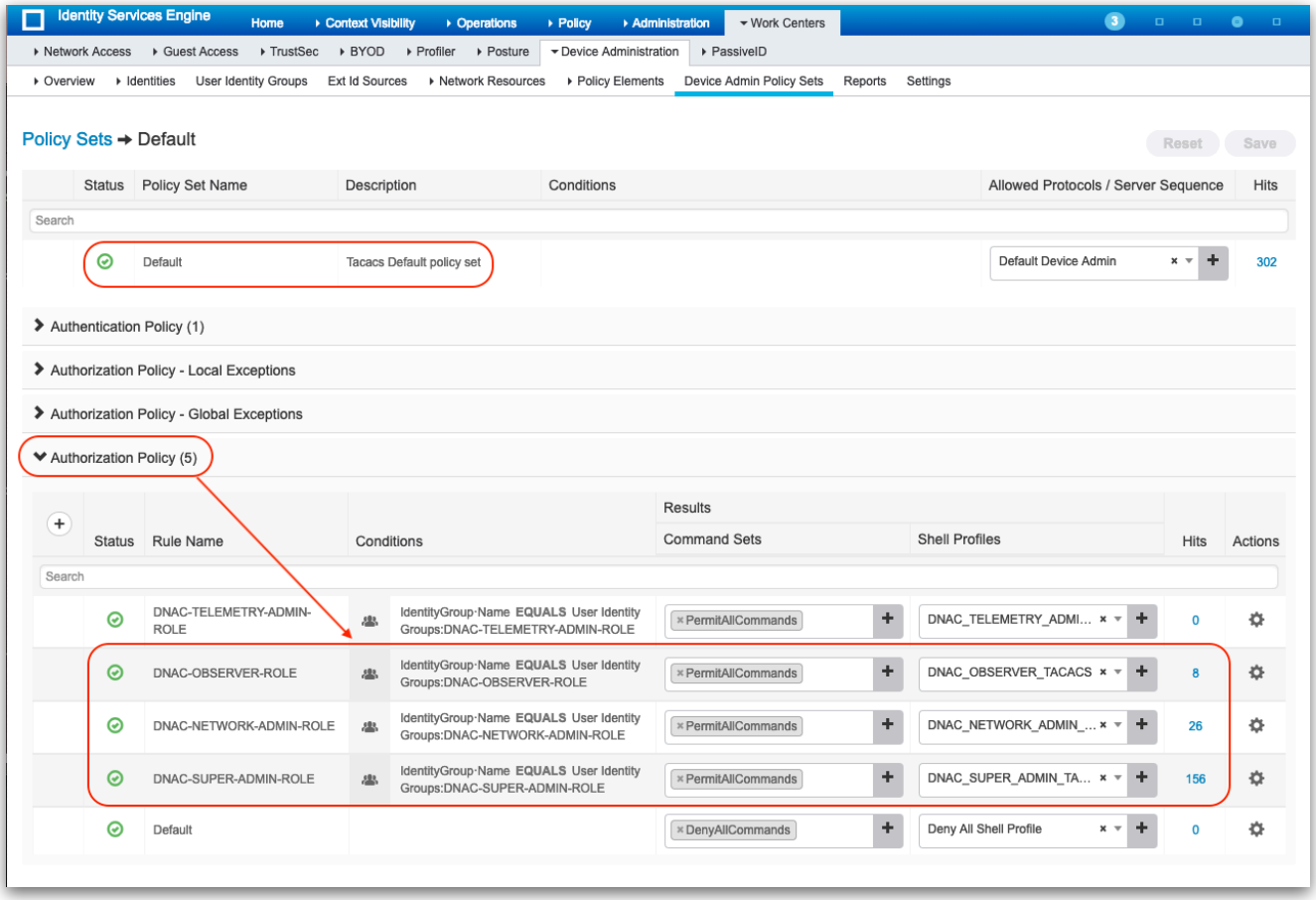


"**Authentication Policy**"

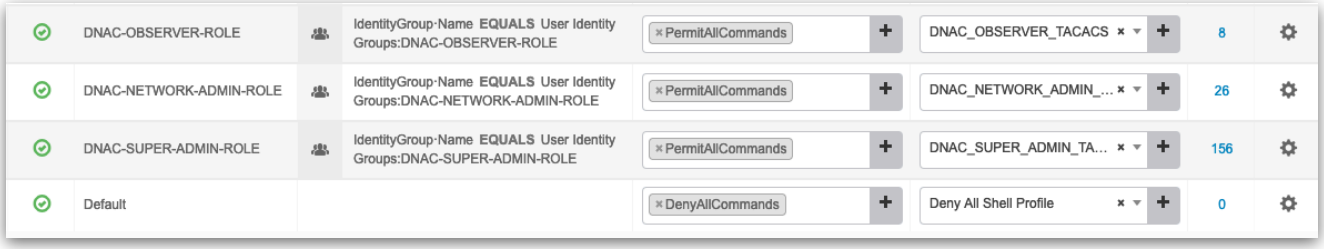
For this example, simply use the "**Default**" Authentication Policy



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



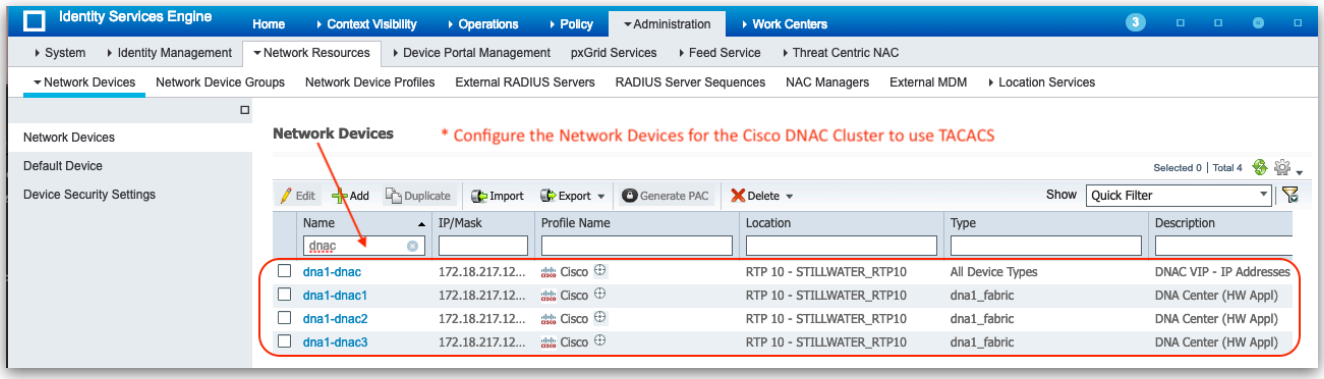
As part of condition, associate to users. These **users** will be created as shown in **step 6.**



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

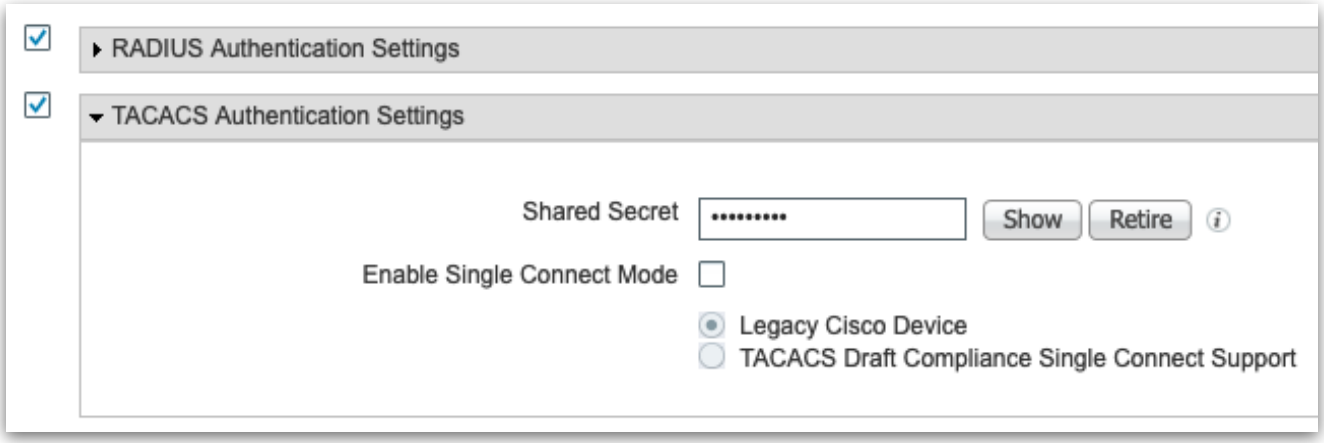
Under **Administration → Network Resources → Network Devices,** select the defined Cisco DNAC Device entries**.**

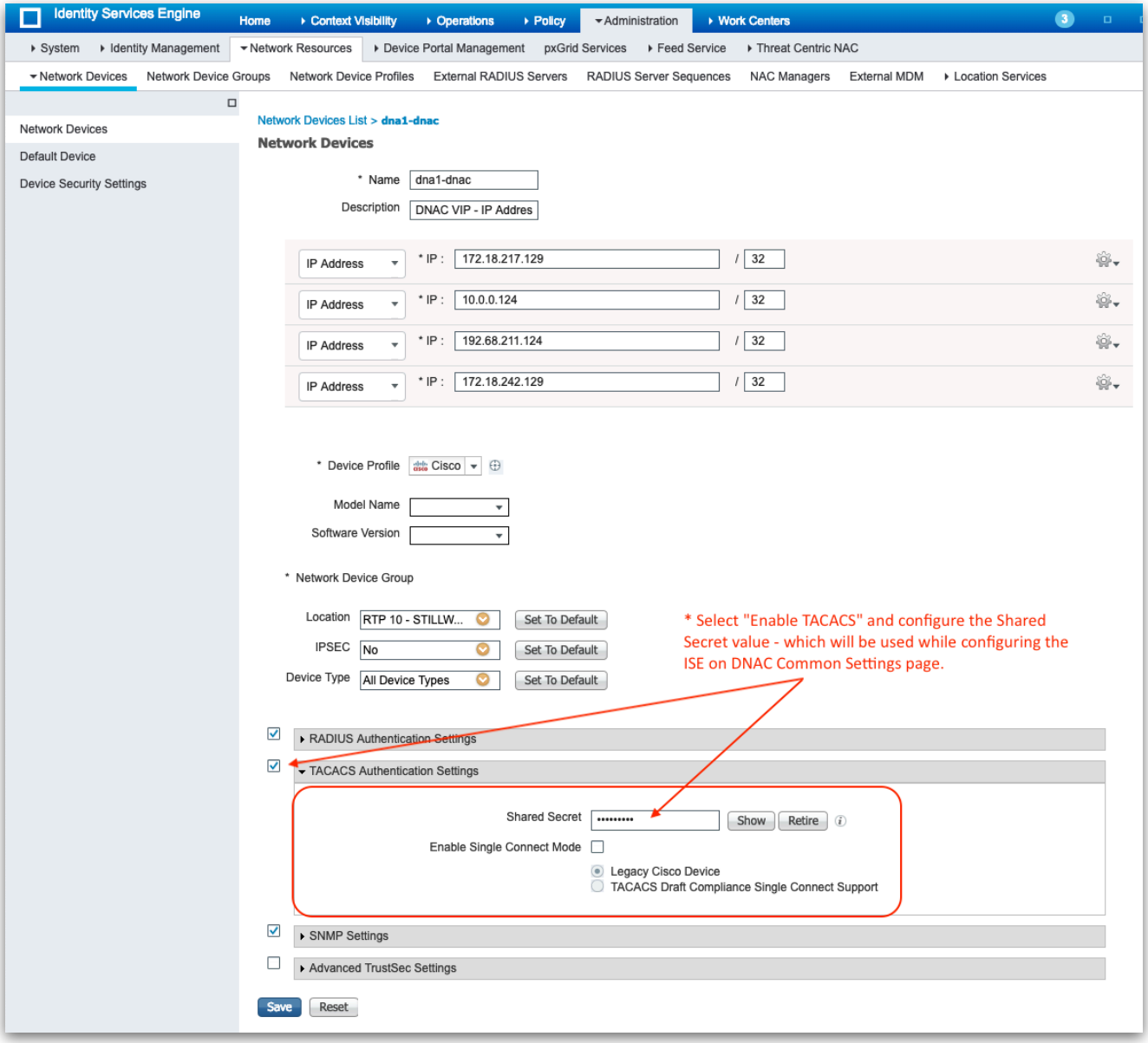
Note: *If a Network Device is not present, Add a Network Device for "each" Cisco DNAC in the Cluster. In addition, Add a Network Device for the Virtual IPs (VIPs).*



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.

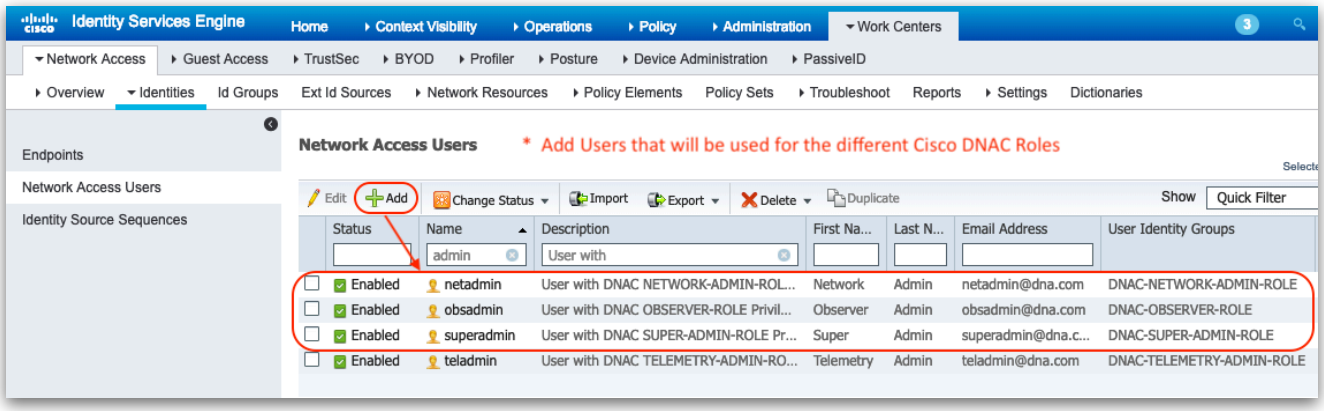
If specific device/IP address entries are present in "Network Devices" tab, enable TACACs settings there as well.



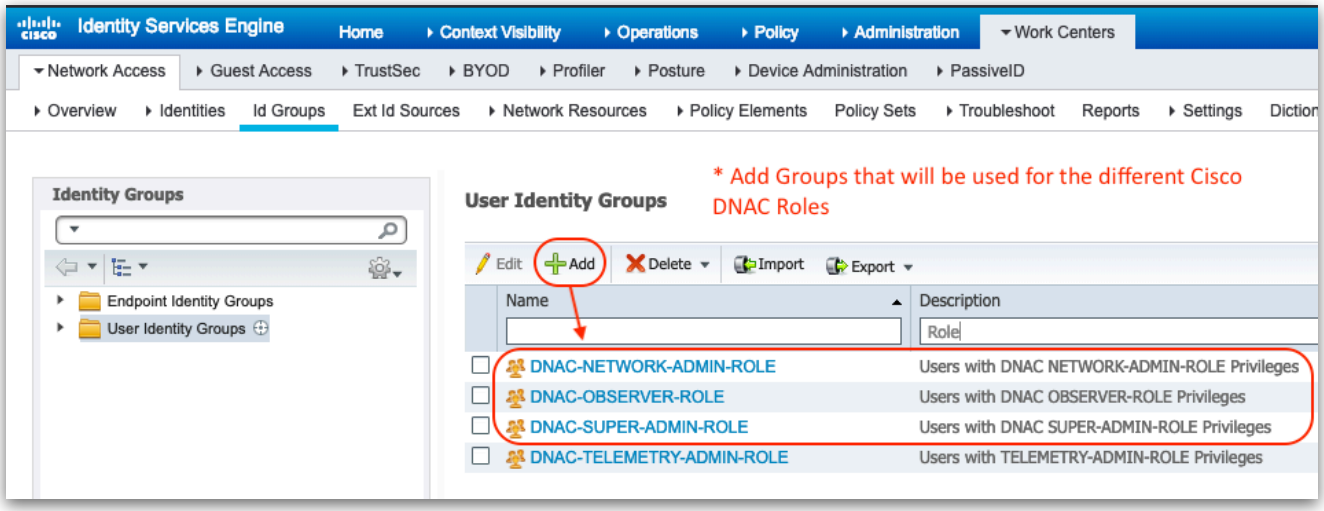

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
Threat Centric NAC
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
NAC Managers
External MDM
Location Services
Network Devices
Default Device
Device Security Settings
Network Devices List > dna1-dnac
Network Devices
* Name dna1-dnac
Description DNAC VIP - IP Addres
IP Address * IP : 172.18.217.129 / 32
IP Address * IP : 10.0.0.124 / 32
IP Address * IP : 192.68.211.124 / 32
IP Address * IP : 172.18.242.129 / 32
* Device Profile Cisco
Model Name
Software Version
* Network Device Group
Location RTP 10 - STILLW... Set To Default
IPSEC No Set To Default
Device Type All Device Types Set To Default
* Select "Enable TACACS" and configure the Shared Secret value - which will be used while configuring the ISE on DNAC Common Settings page.
RADIUS Authentication Settings
TACACS Authentication Settings
Shared Secret ••••••••• Show Retire
Enable Single Connect Mode
Legacy Cisco Device
TACACS Draft Compliance Single Connect Support
SNMP Settings
Advanced TrustSec Settings
Save Reset

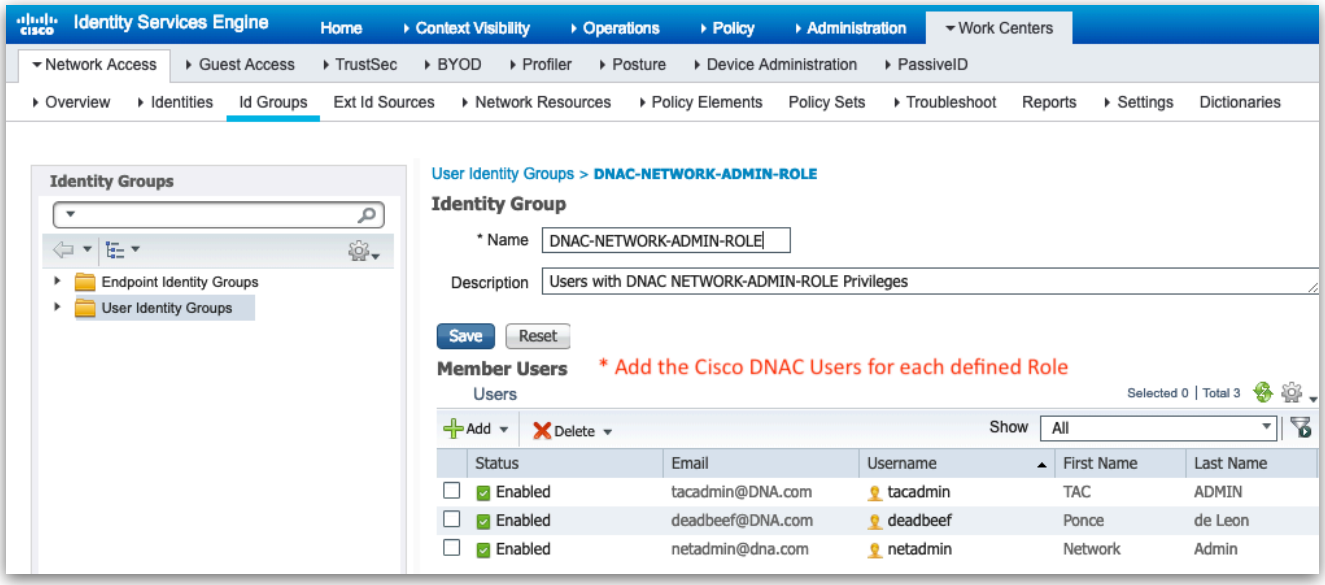
- **Step 6: Add Users & Groups that will be used for the different Cisco DNAC Roles**

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 :



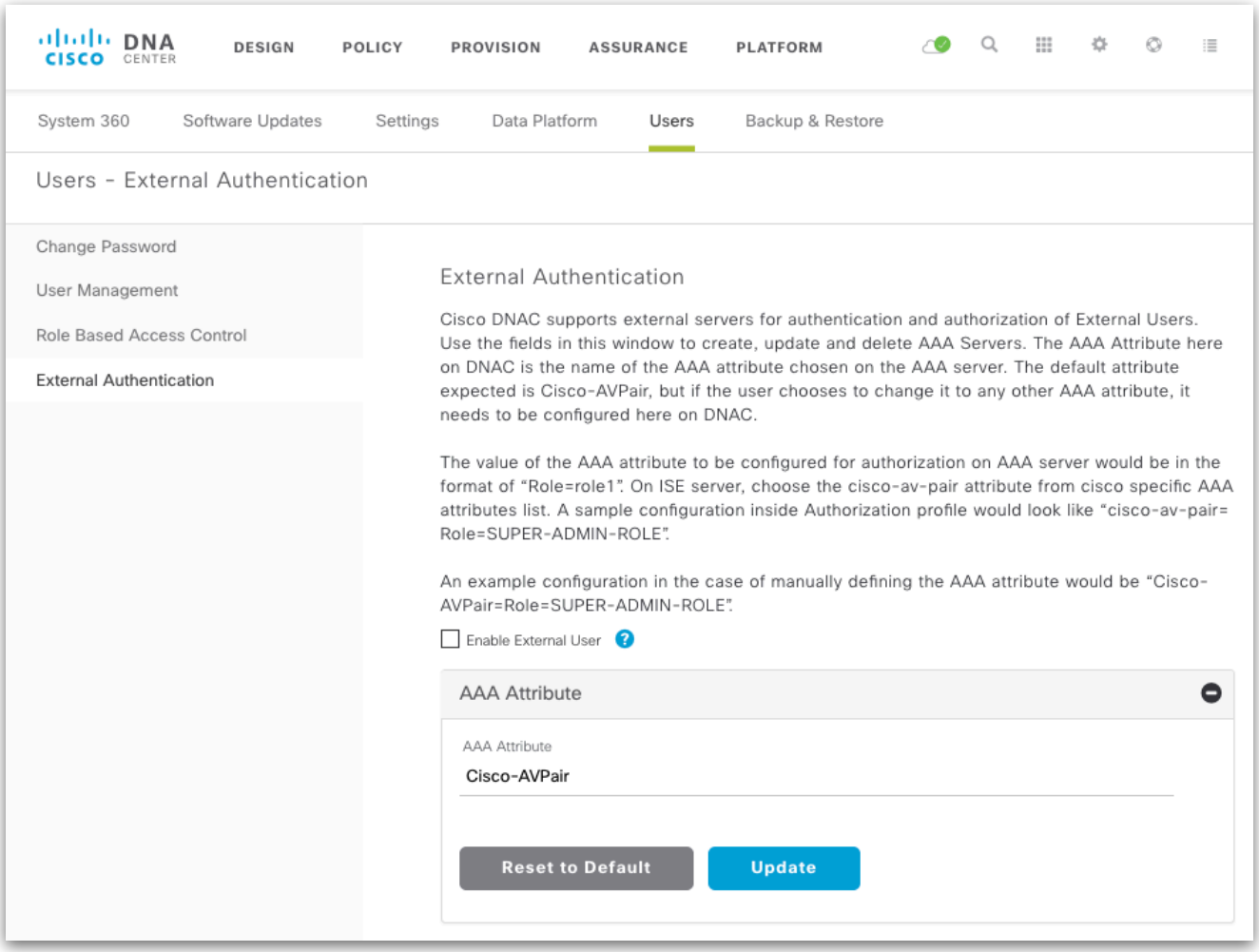

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Identities
Id Groups
Ext Id Sources
Network Resources
Policy Elements
Policy Sets
Troubleshoot
Reports
Settings
Dictionaries
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups > DNAC-NETWORK-ADMIN-ROLE
Identity Group
* Name
DNAC-NETWORK-ADMIN-ROLE
Description
Users with DNAC NETWORK-ADMIN-ROLE Privileges
Save
Reset
Member Users
* Add the Cisco DNAC Users for each defined Role
Users
Selected 0 | Total 3
Add
Delete
Show
All
Status
Email
Username
First Name
Last Name
Enabled
tacadmin@DNA.com
tacadmin
TAC
ADMIN
Enabled
deadbeef@DNA.com
deadbeef
Ponce
de Leon
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**

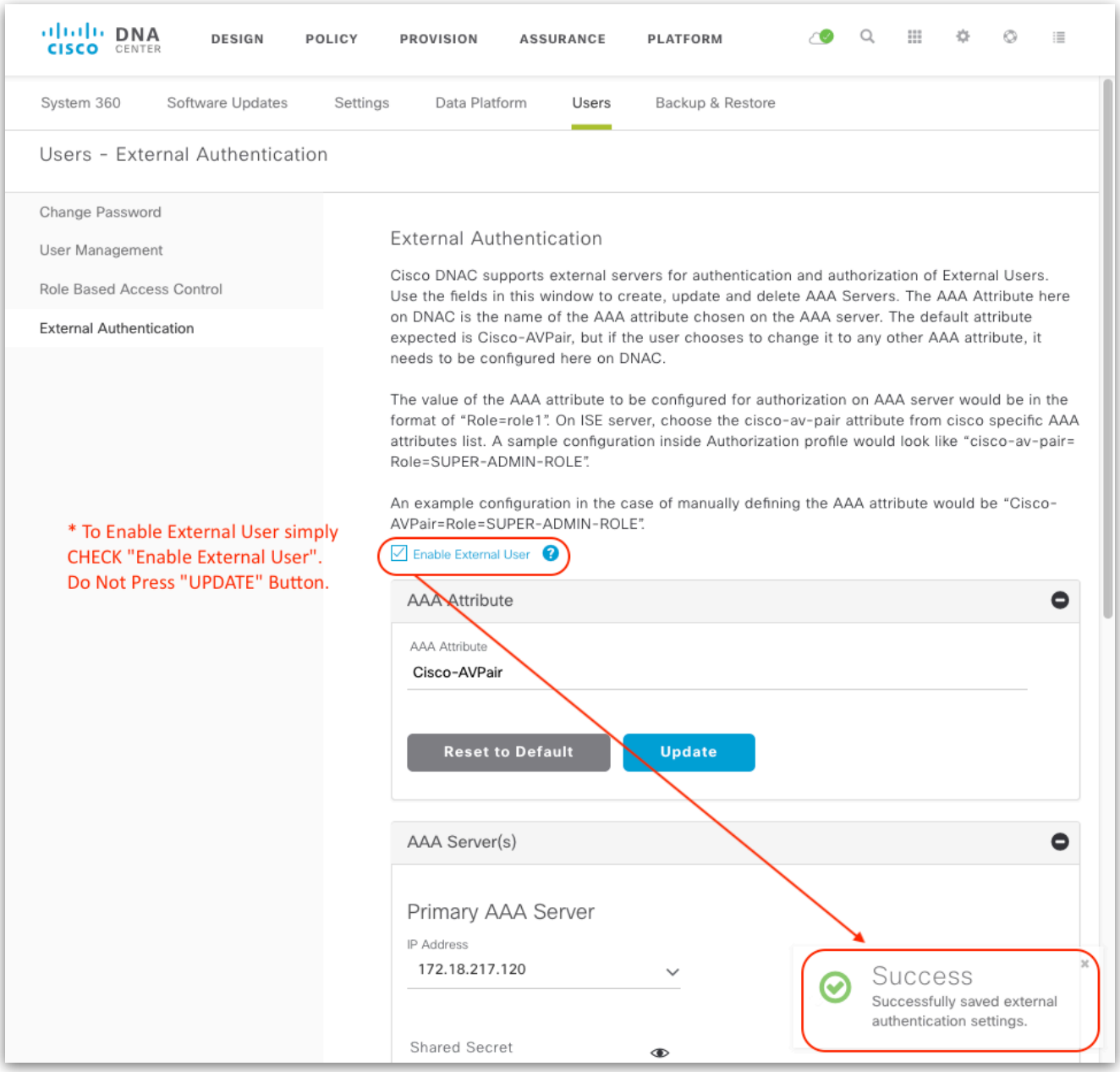
This task is important to pay attention to each step that you perform when enabling external authentication. **The AAA Attribute value for "cisco av pair" can change based on an action that you perform.** The AAA Attribute value that you configured in TASK_2 needs to match what the Cisco DNAC is expecting for the authentication credentials exchange.

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



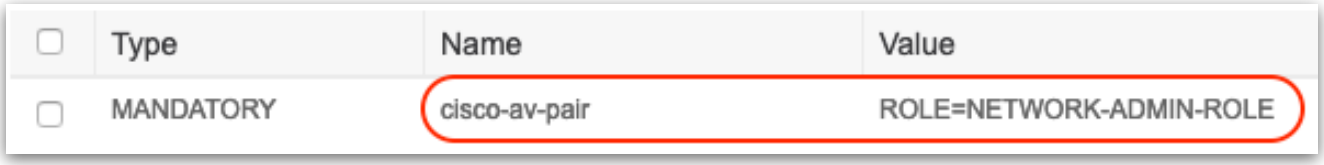
- **Step 1: Enable External User Authentication**

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.***"



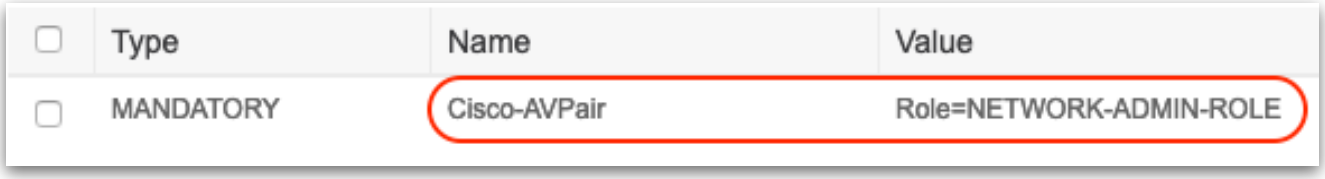
If you checked "**Enable External User**" and **Do Not Press "UPDATE" Button**, the following is the syntax used when configuring the ISE TACACS Profile. This is the **"Original" DEFAULT** AAA Attribute value.

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



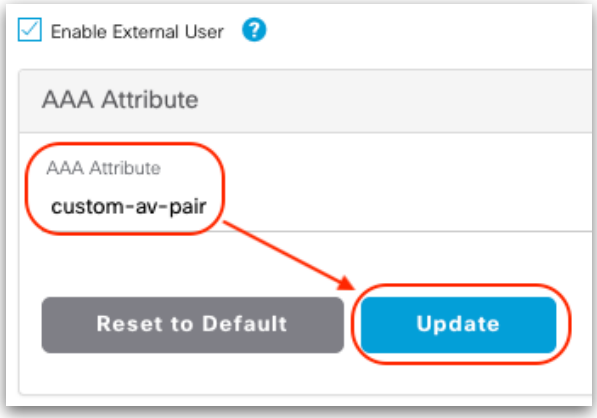
Gotcha_1: If you checked "**Enable External User**" and then **Pressed "UPDATE" Button**, the following is the syntax used when configuring the ISE TACACS Profile. This is the **"New" DEFAULT** AAA Attribute value.

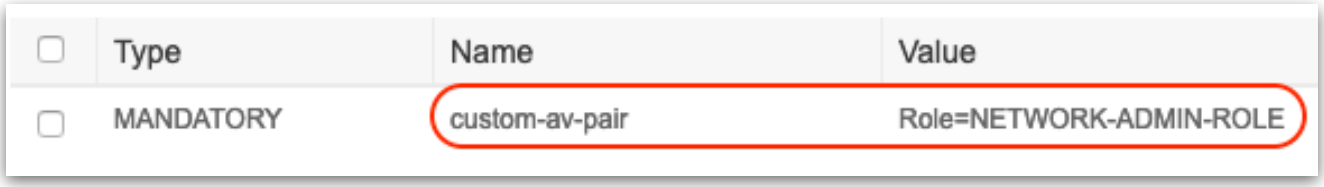
Cisco-AVPair **Role=NETWORK-ADMIN-ROLE**



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.

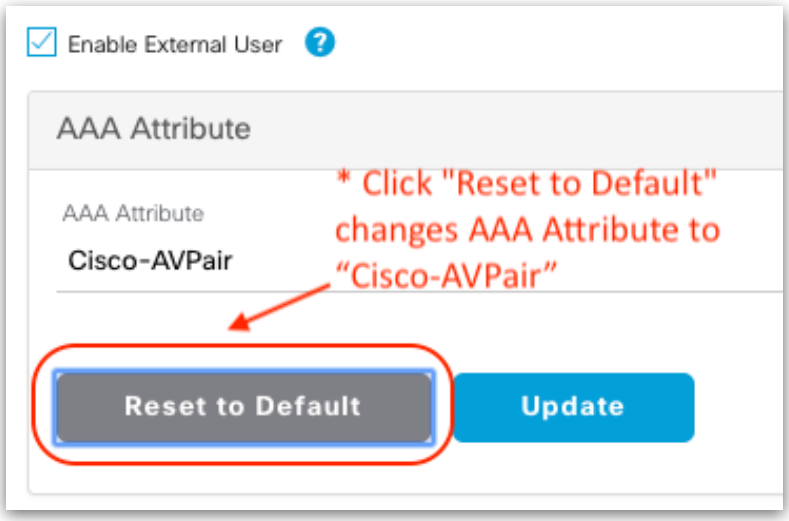
custom-av-pair **Role=NETWORK-ADMIN-ROLE**

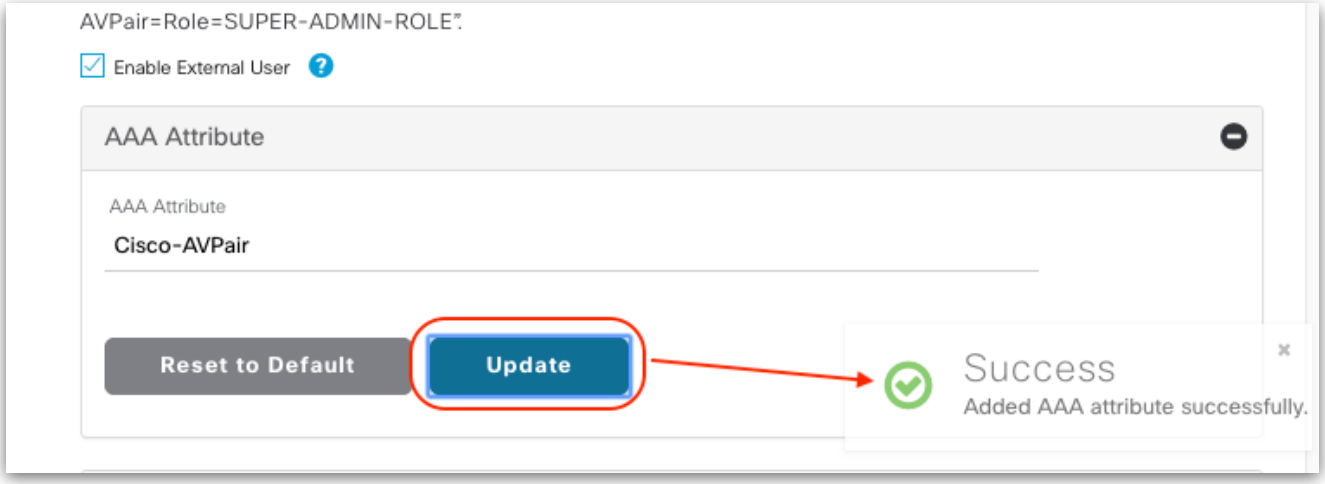




Gotcha_2: If you changed the AAA Attribute to and you want to **reset** the AAA Attribute **BACK TO THE DEFAULT** value, perform the following:

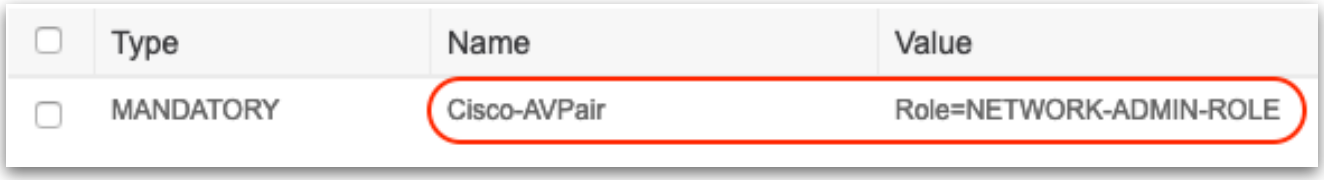
- Click "**Reset to Default**"
- Click "**Update**"





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



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

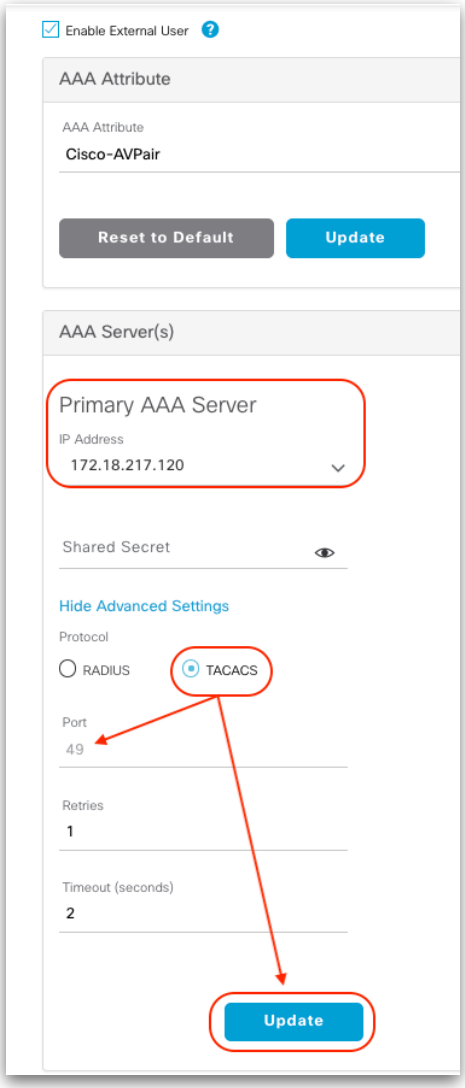
✓ Under the AAA Server(s) section, select the ISE Server.

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

✓ Select TACACS Protocol.

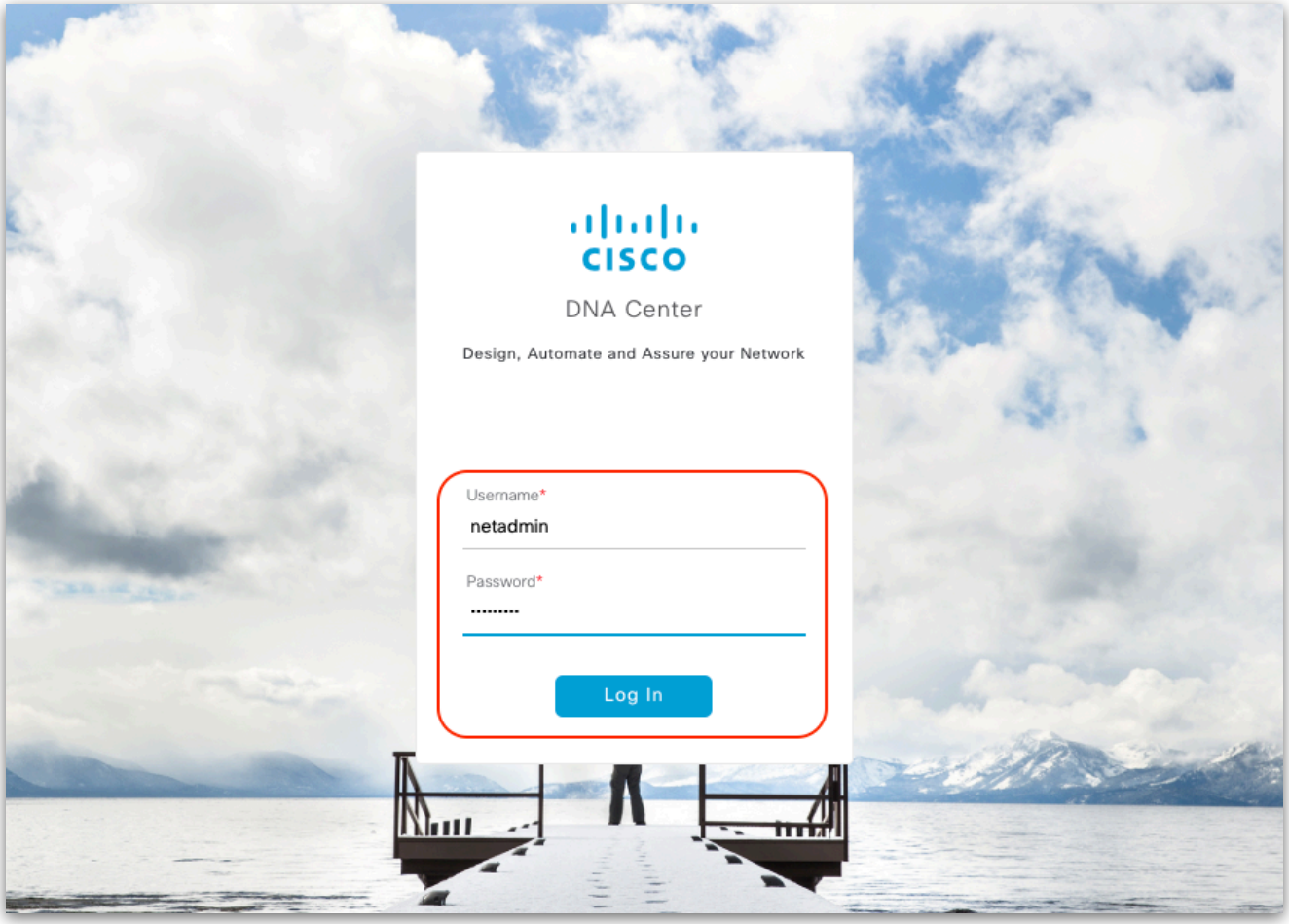
Note: *The TACACS protocol port number is 49. This is not configurable in Cisco DNAC version 1.2.8 or later.*

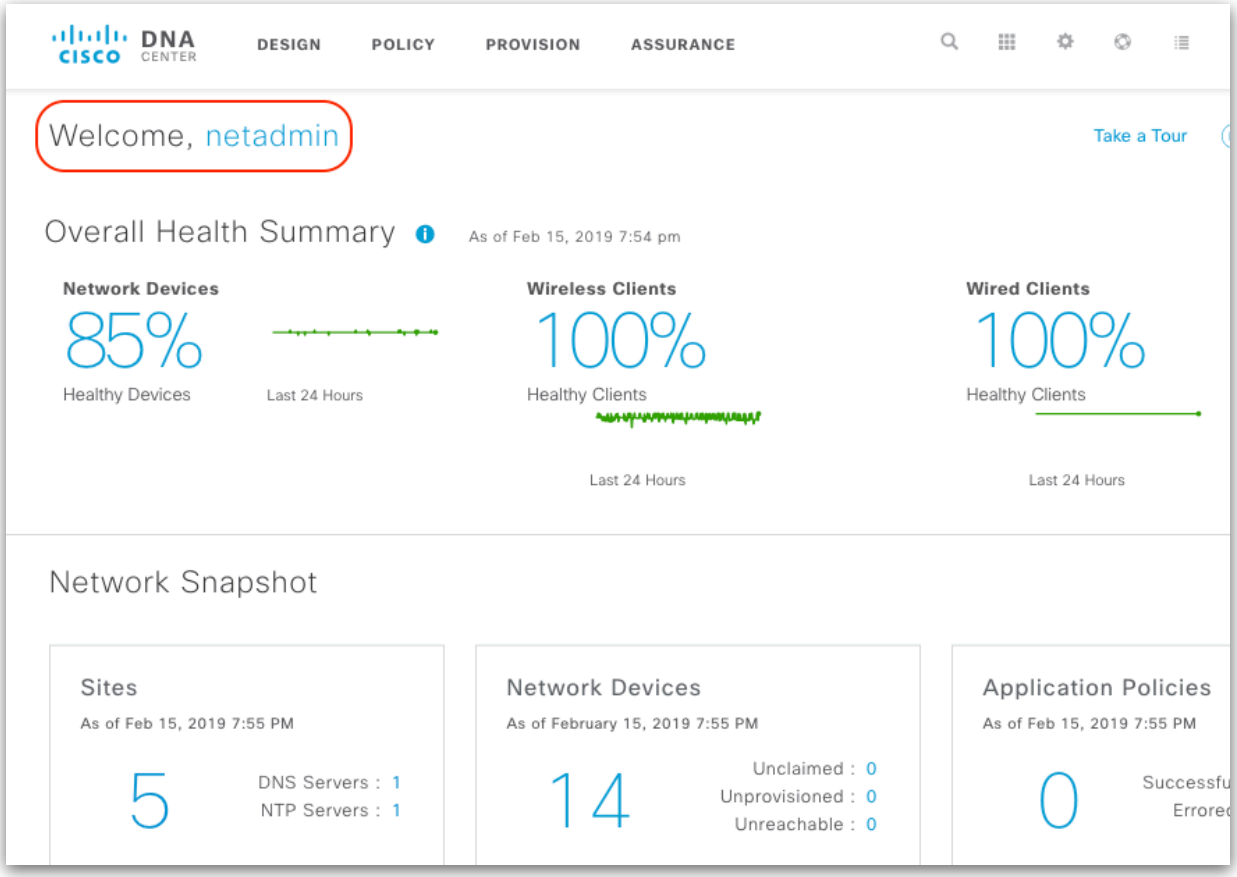
✓ Click UPDATE to save changes



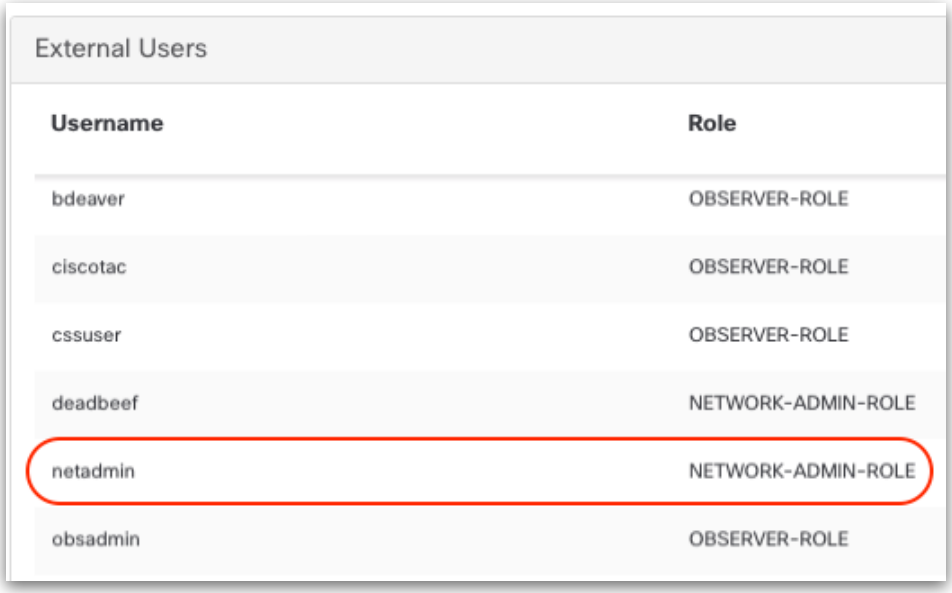
TASK_4 - VERIFY CISCO DNAC USER MANAGEMENT FOR EXTERNAL AUTHENTICATION USING TACACS WITH CISCO ISE.

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



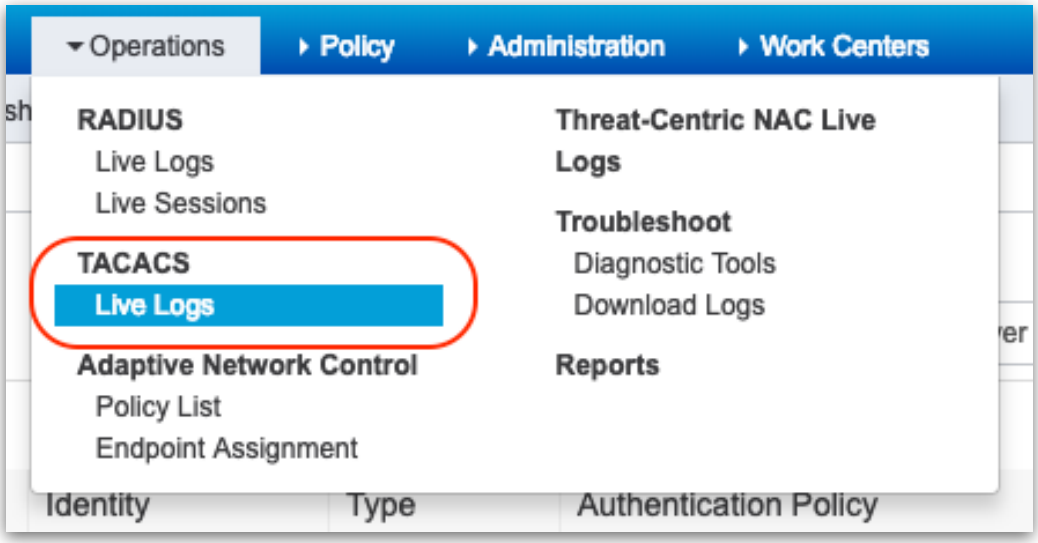


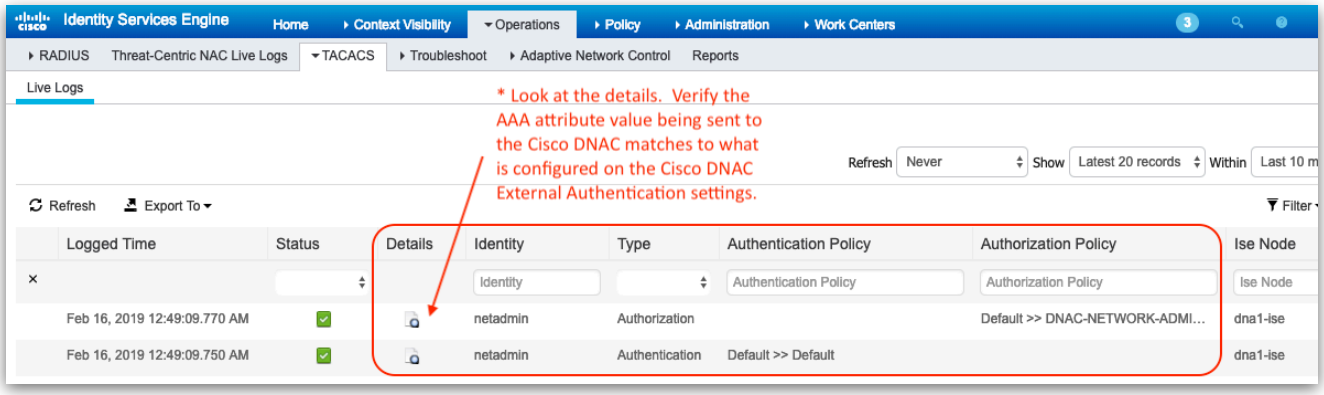
- From the Cisco DNAC GUI, Goto -> **System Settings-> Users-> External Authentication**
  Look at the External Users list. You should see the TACACS users listed and their assigned roles.



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

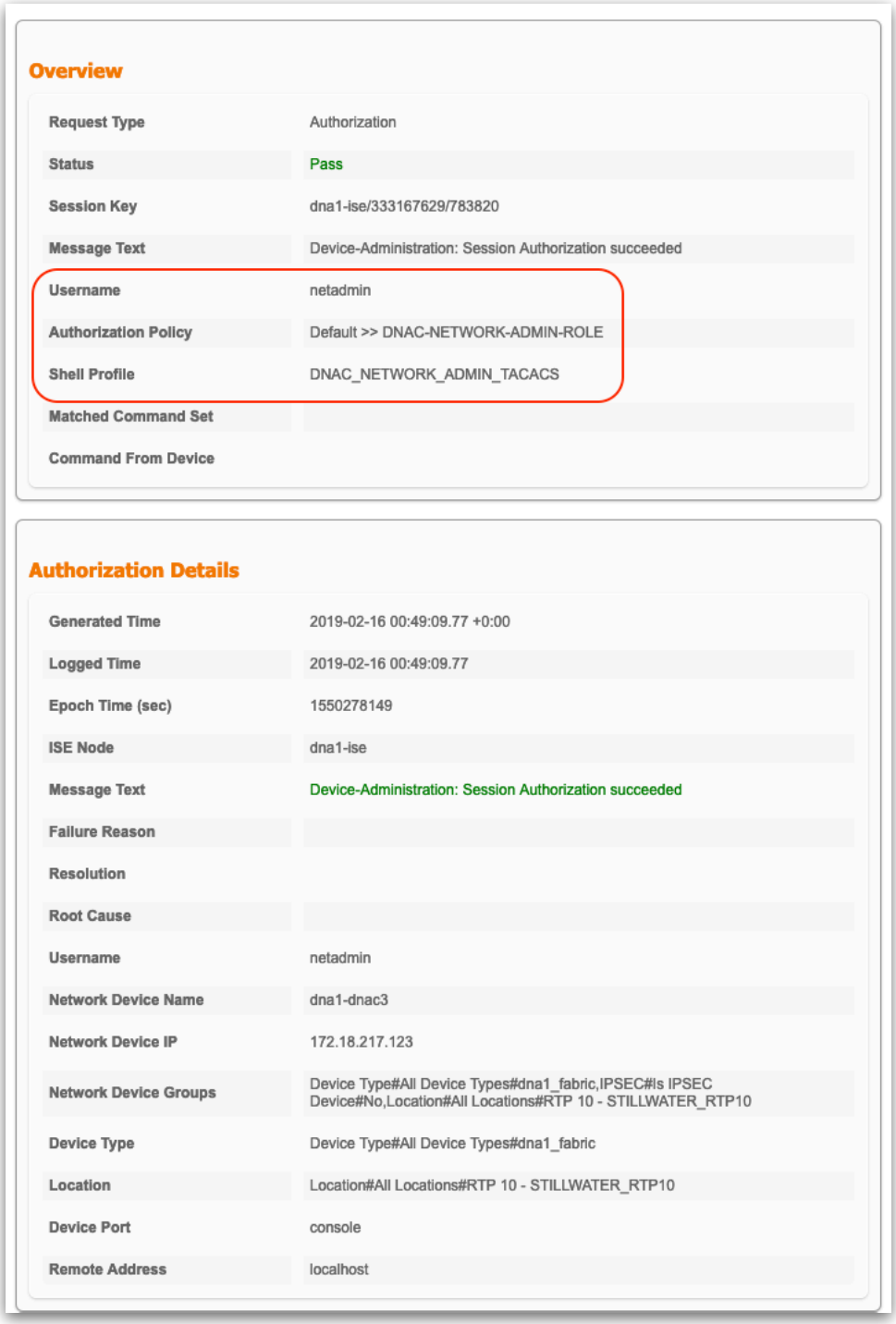
13005	Received TACACS+ Authorization Request
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15041	Evaluating Identity Policy
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore
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 Attribues	
All Response Attribues	Cisco-AVPair=Role=NETWORK-ADMIN-ROLE,priv-lvl=15

TACACS Protocol

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

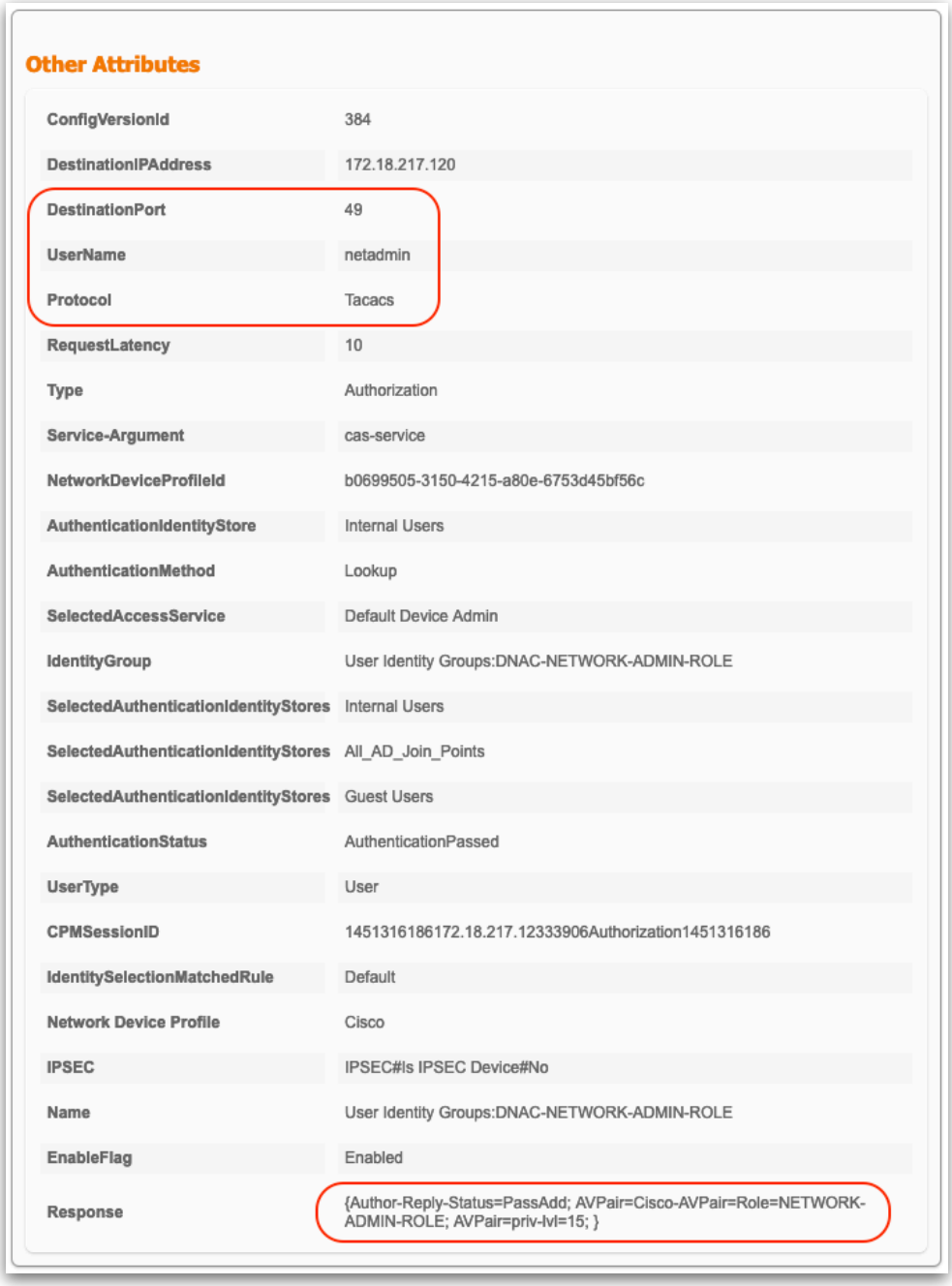


Overview

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 -RHIrnis "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.maglev.identitymgmt.api.TokenEndPoint","message":"**JWT token is generated successfully.**","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":31,"threadPriority":5}

{"timeMillis":
1550281951650,"thread":"qtp864326906-31","level":"INFO","loggerName":"com.cisco.maglev.identitymgmt.api.TokenEndPoint","message":"**Cookie is set successfully.**","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":31,"threadPriority":5}

{"timeMillis":
1550281951651,"thread":"qtp864326906-31","level":"INFO","loggerName":"com.cisco.maglev.identitymgmt.api.TokenEndPoint","message":"**'netadmin' logged in successfully.**","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":31,"threadPriority":5}

{"timeMillis":
1550281953112,"thread":"qtp864326906-32","level":"INFO","loggerName":"com.cisco.maglev.sdk.persistence.document.BaseDocumentDao","message":"The number of entities found is
15","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":32,"threadPriority":5}
timeMillis":
1550281951651,"thread":"qtp864326906-31","level":"INFO","loggerName":"com.cisco.maglev.identitymgmt.api.TokenEndPoint","message":"**'netadmin' logged in successfully.**","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":31,"threadPriority":5}

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