TACACS+ W/ CISCO ISE AND AOS-CX

CONTENTS

REQUIREMENTS

- Aruba Switch (6300,6400)
- Cisco ISE (2.3 And Above)

OVERVIEW

This document will cover how to configure TACACS with AOS-CX.

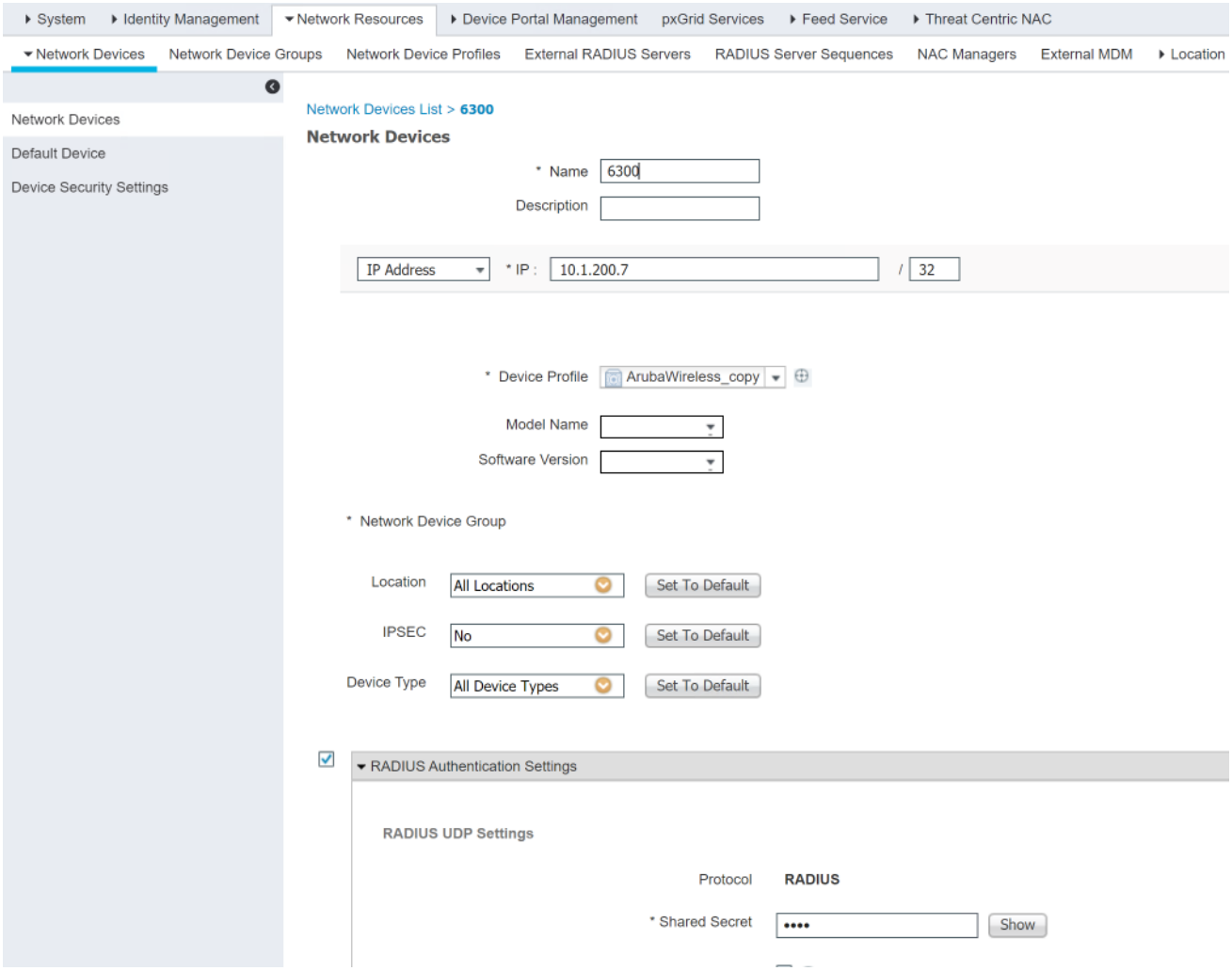
In this scenario, we will create a local user “Joe_admin” Admin TACACS user locally with ISE and restrict the commands so that the “Joe_admim” can use. This document will also show how to verify the user has successfully logged in and can use the authorized commands.

ADDING DEVICES TO CISCO ISE

To Add a device to Cisco ISE navigate to “Administration>Network Resources> Devices” Click Add device.

- Enter the Device IP
- Select the Device Profile that was just created (In this case “ArubaWireless_copy”)
- Enter the shared secret

Note: The “ArubaWireless” profile will also work for TACACS this profile was created order to work with Radius. Guide for how to get Radius working with Cisco ISE [Here]



Switch Configuration

Global AAA Configuration.

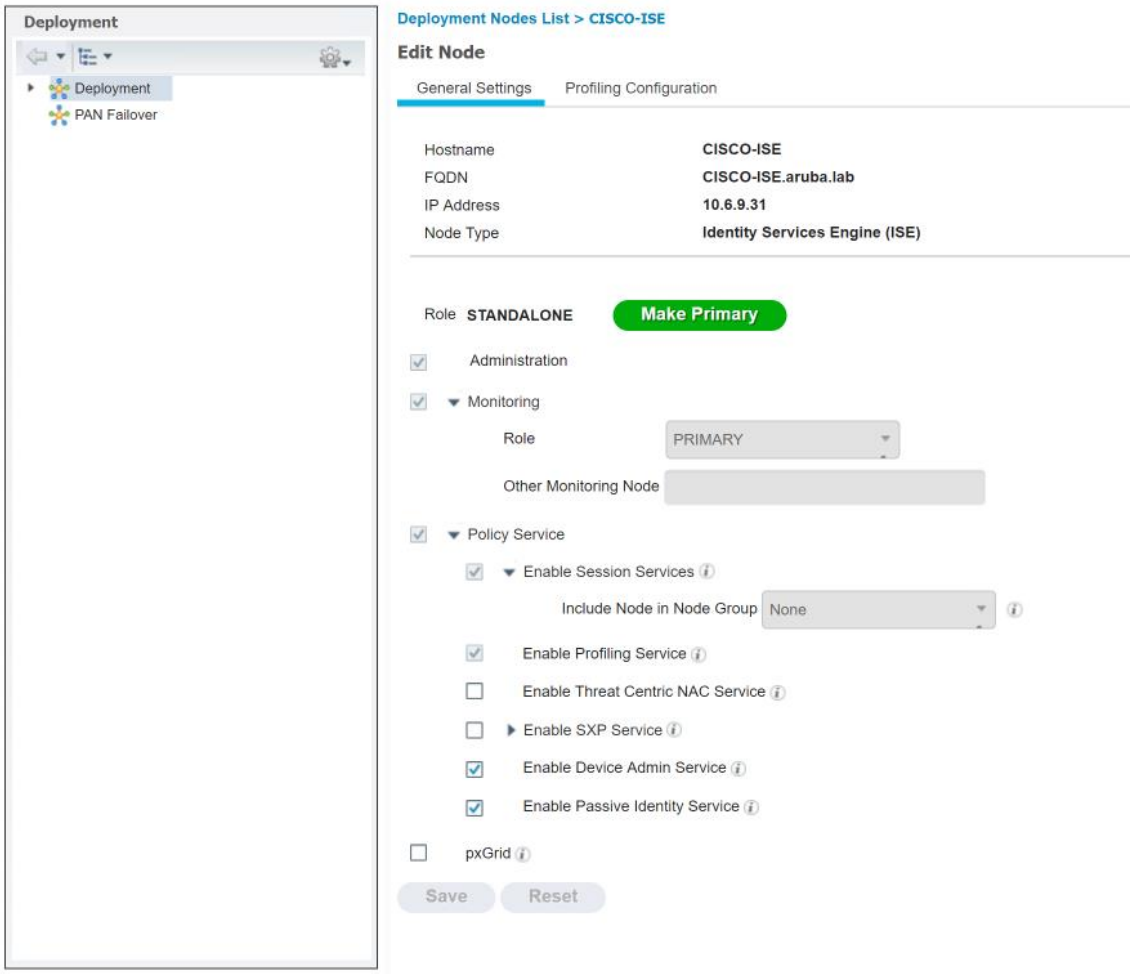
```
tacacs-server host <TACACS-IP> key Plaintext <key>
aaa group server tacacs <group-name>
    server <TACACS-IP>
aaa authentication login ssh group <TACACS Server Group Name> local
aaa authorization commands default group <TACACS Server Group Name> local
aaa accounting all default start-stop group <TACACS Server Group Name> local
```

ENABLING TACACS IN CISCO ISE

Description

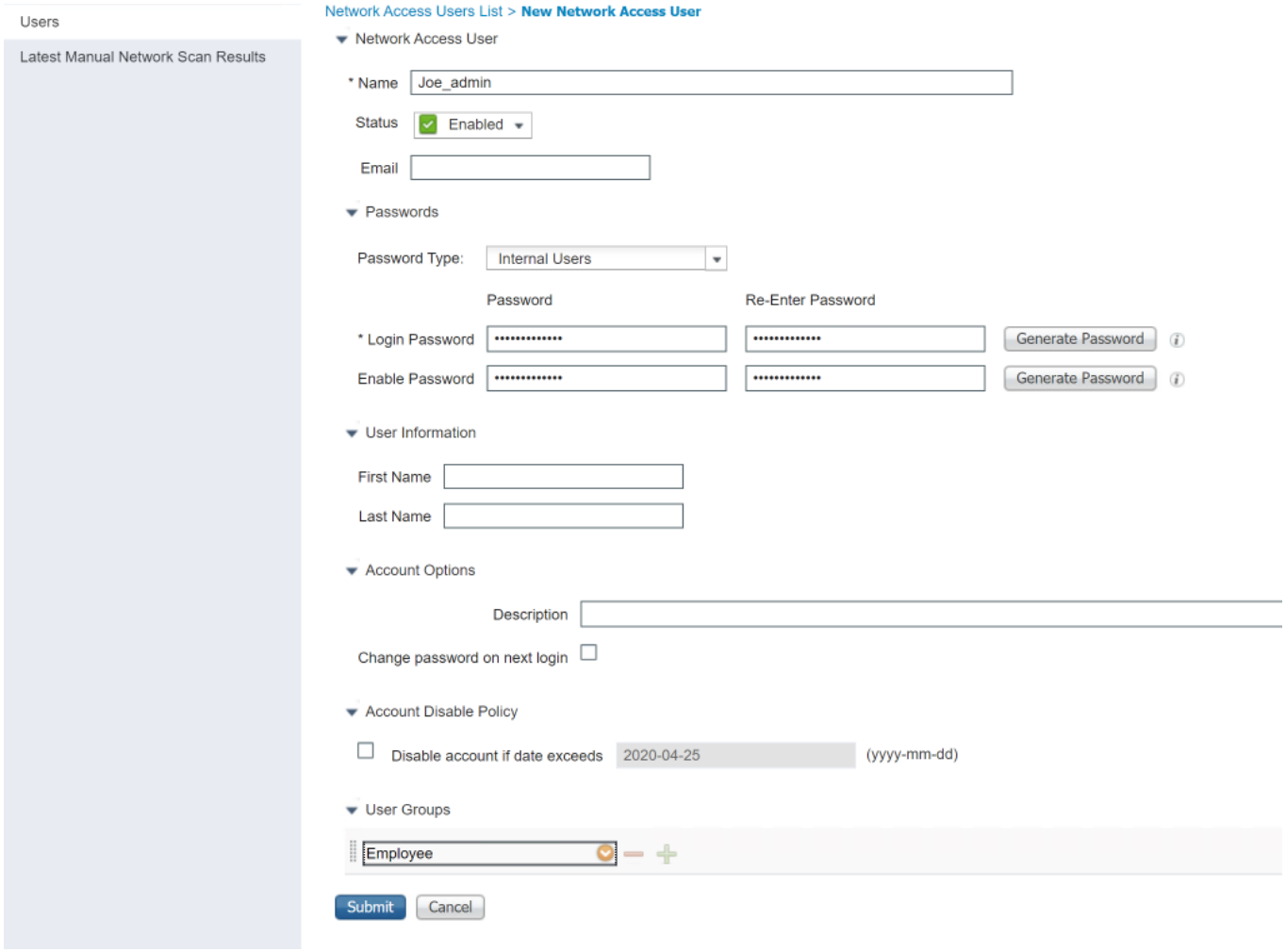
This section will show how to enable the TACACS service within Cisco ISE this section will also go over creating a user and user groups.

1. Navigate to “Administration>System>Deployment” Check the “Enable Device Admin Service” and “Enable Passive Identity Service” boxes.

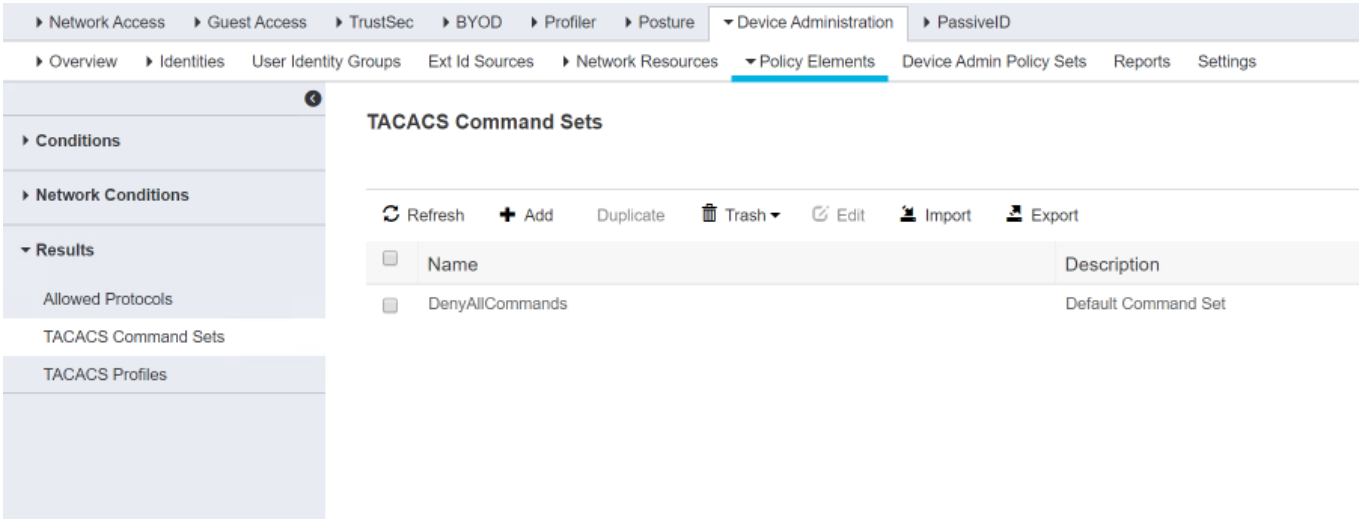


2. Next Create a user Navigate to “Administration> Identity Management> Identities” and Click “+ Add”

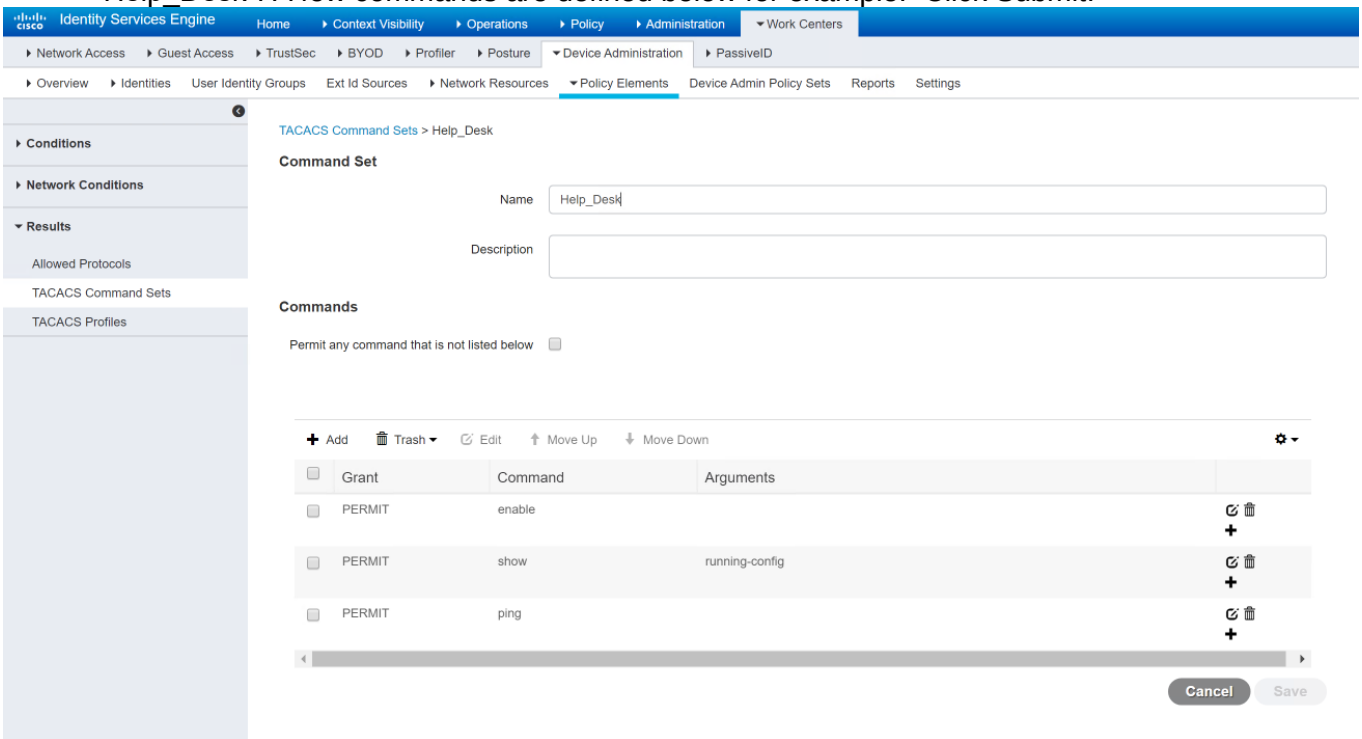
   Set the login password and enable password also set the user to the proper group in this case it will be the “Employee” Group



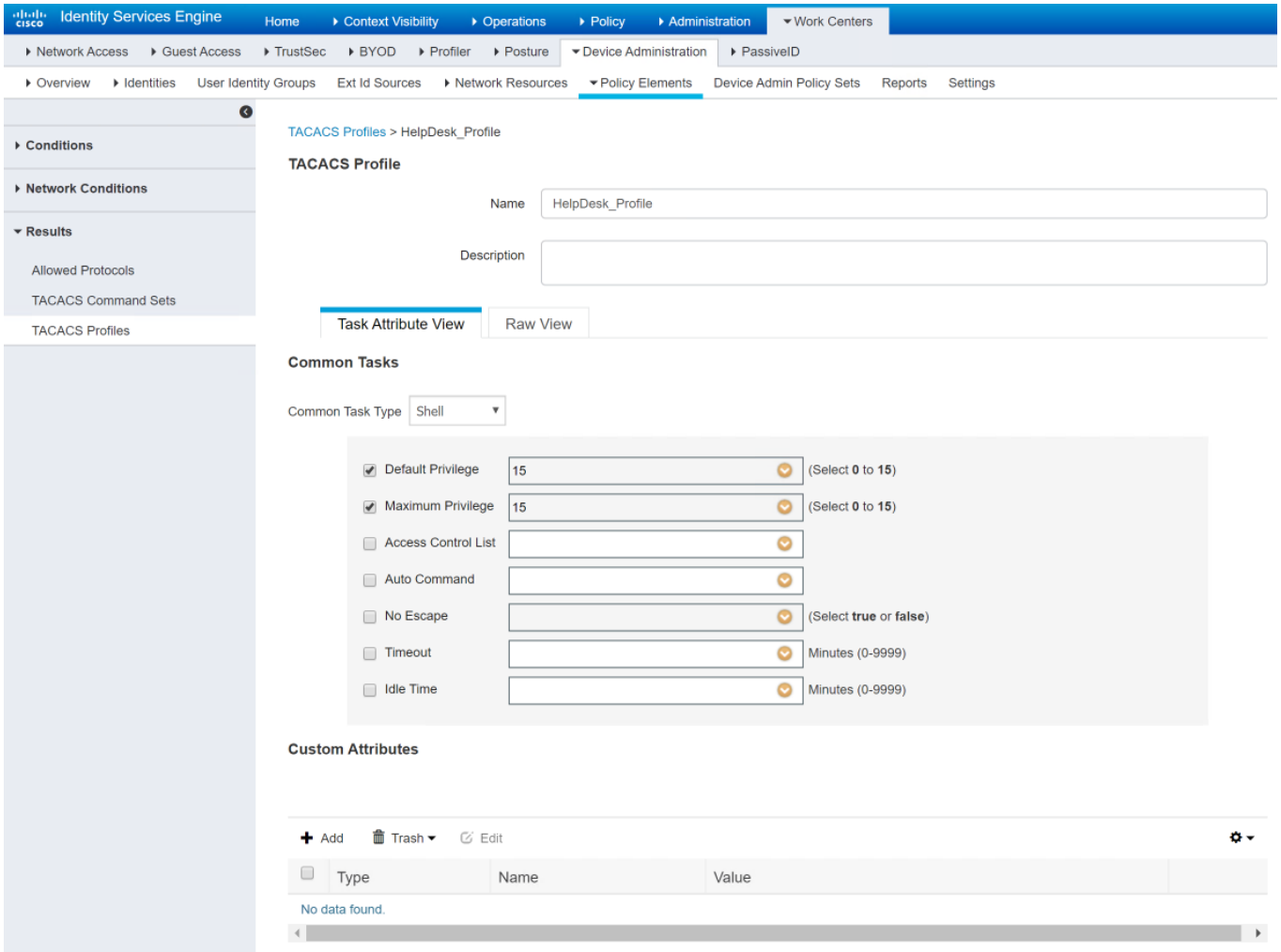
3. Next is to restrict the amount of command that Joe_Admin can use. Navigate to “Work Centers> Device Administration> Policy Elements” Click Results and “Command sets” Click Add to add another command set



4. All the commands that the Joe_Admin can use will be defined in the command set named “Help_Desk”. A few commands are defined below for example. Click Submit.



5. Next a profile has to be configured this profile will be named “HelpDesk_Profile”. This is used to set the privileged level on the AOS-CX switch. This needs to be set to 15, but based on the command set, it will permit/Deny the user to use certain commands. Navigate to “Work Centers>Device Administration>Policy Elements”
   “Results >TACACS Profiles”
   “Click Add”



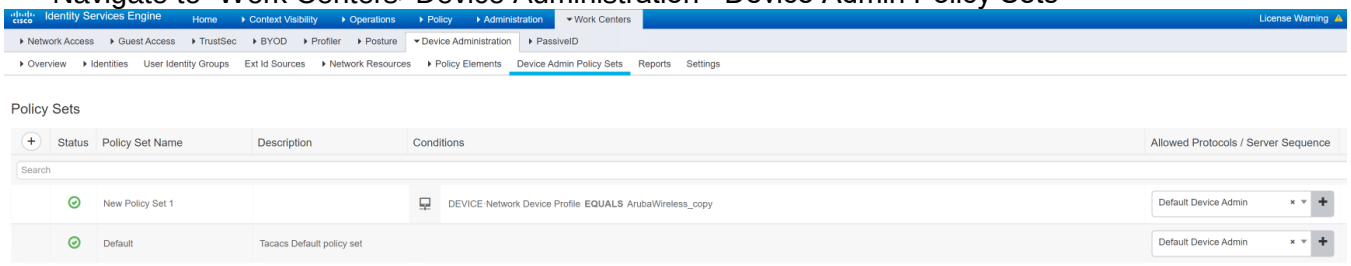
CREATING A TACACS POLICY

Description

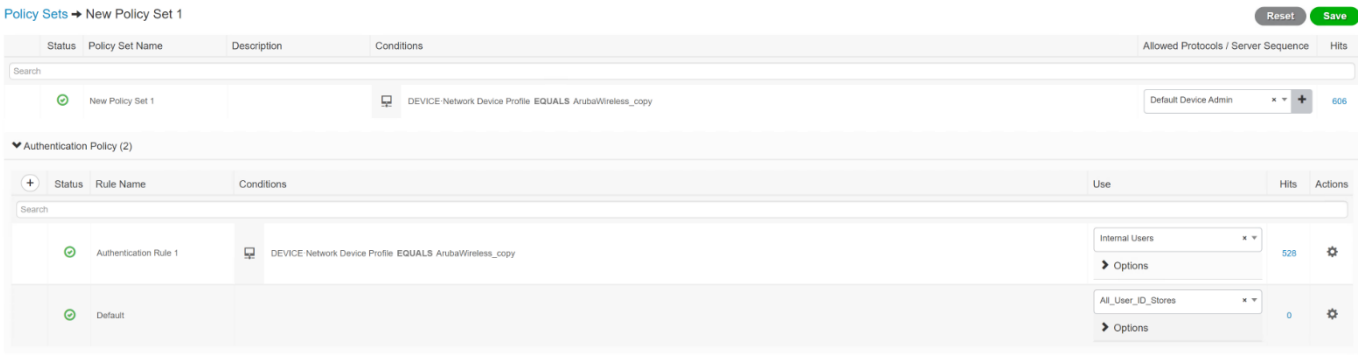
This section will go over how to create a TACACS policy.

1. Create a policy for a TACACS rule, the rule, in this case, is set to match on the devices in the Device Profile “ArubaWireless_Copy”. This is set under the device type when adding a device into ISE.

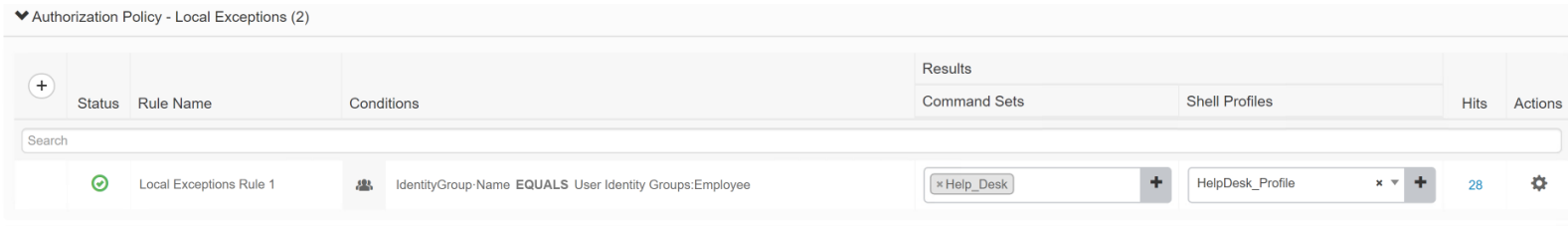
Navigate to “Work Centers>Device Administration> Device Admin Policy Sets”



2. Set the authentication mechanism in this case its set to internal users

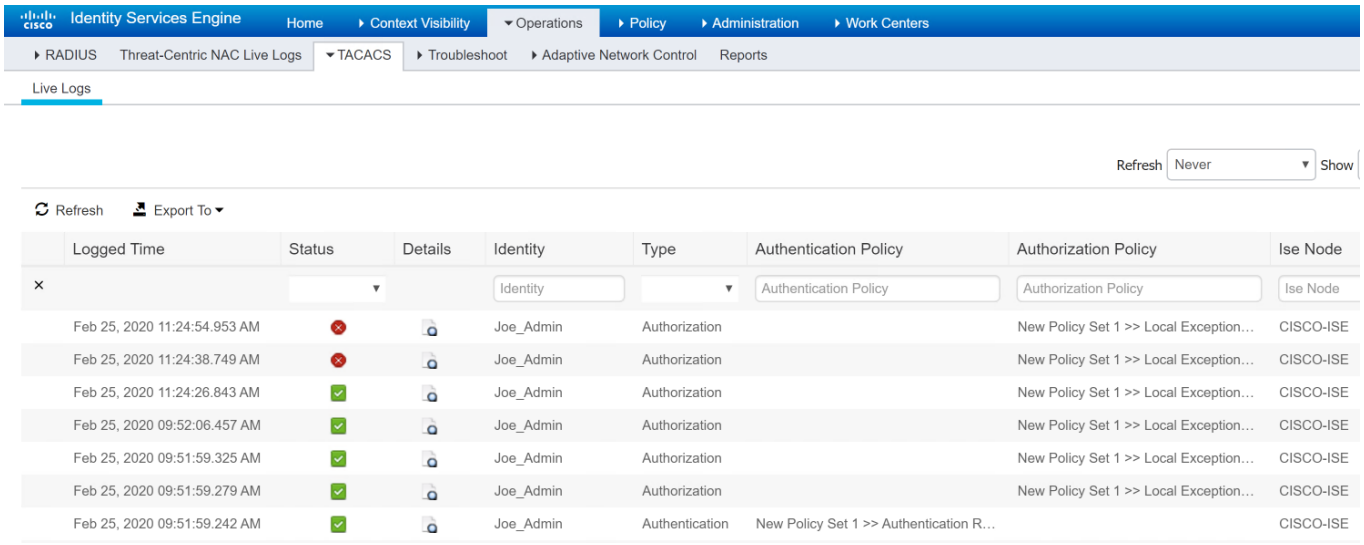


3. Create an Authorization policy and in this set up it the condition to trigger the authorization command set and profile will be the User Identity Group of “Employee**”**. The command set result will be the “Help_Desk” as well, the profile will be set to the “HelpDesk_Profile”

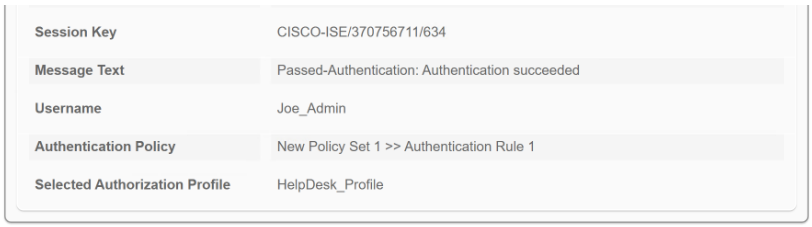


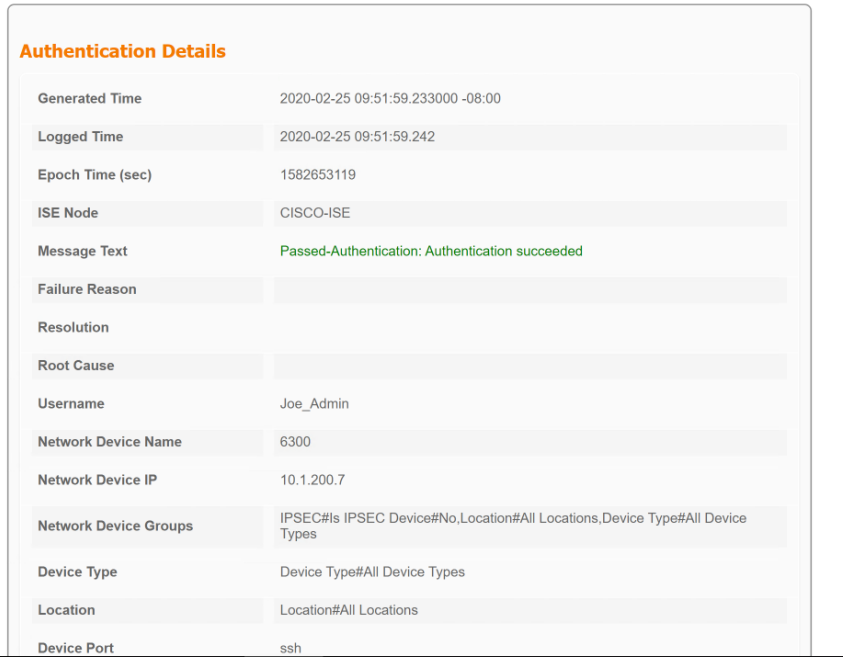
VERIFICATION

1. Using “ISE TACACS Live Logs” the users can be seen logging in.



By clicking the magnified glass, users can drill down into a particular sessions.





2. When the “Joe_Admin” user logs in to the switch, we can see that the user cannot use certain commands as well.