

TACACS+ W/ CISCO ISE AND ARUBAOS-SWITCH

CONTENTS

TACACS+ W/ Cisco ISE and ArubaOS-Switch	. 1
Requirements	. 1
Overview	. 1
Adding a Device To ISE	. 2
Enabling TACACS In Cisco ISE	
Creating a TACACS Policy	10
Verification	

REQUIREMENTS

- Aruba Switch (2930M/F, 3810M, 5400)
- Cisco ISE (2.3 And Above)

OVERVIEW

This document will cover how to configure TACACS with ArubaOS-Switch.

In this scenario, we will create a Jr. Admin TACACS user locally with ISE and restrict the Jr. admins commands so that the admin can ping and show the running configuration of the switch.

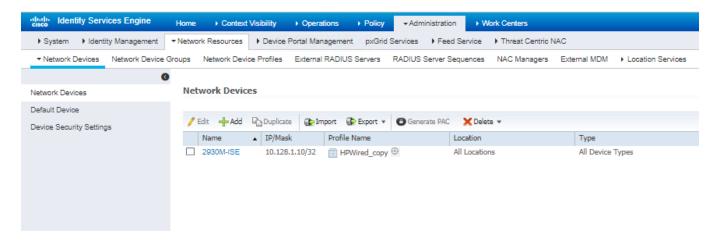


ADDING A DEVICE TO ISE

Description

This section will go over adding a device into Cisco ISE.

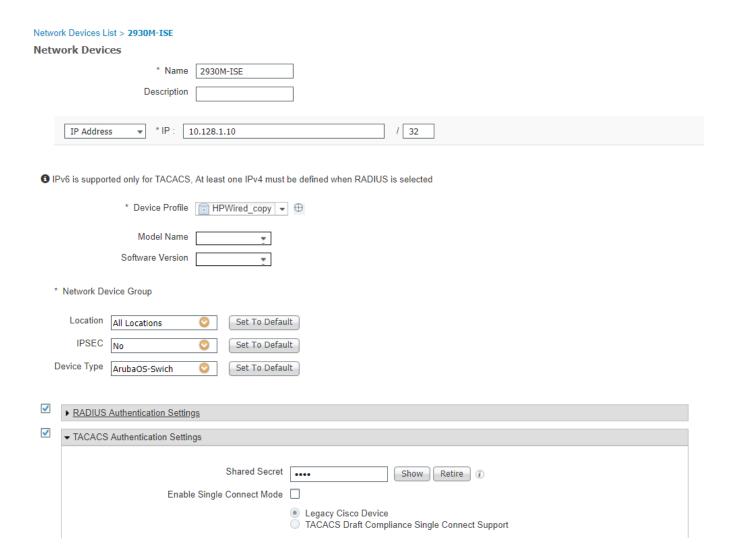
Navigate to "Administration> Network Devices. Click Add."





Enter the IP address, TACACS shared secret, and Model of the switch and select the proper switch profile. Set the device type to something that can be used to group devices in this case we created "ArubaOS-Switch" this will be used later when setting up the policy.

In this example, a copy of the HPWired Profile "HPWired _Copy" is being used, there is no issues using the default HPWired Profile this will work for TACACS as well.





Switch Configuration

TACACS Switch configuration

```
password manager user-name <name> plaintext <password>

TACACS-server host <IP-Address> key <key>
TACACS-server timeout 50

TACACS-server dead-time 20

aaa authentication console login TACACS local
aaa authentication console enable TACACS local

aaa authentication ssh login TACACS local
aaa authentication ssh enable TACACS local

aaa authentication login privilege-mode
aaa authorization commands tacacs
```

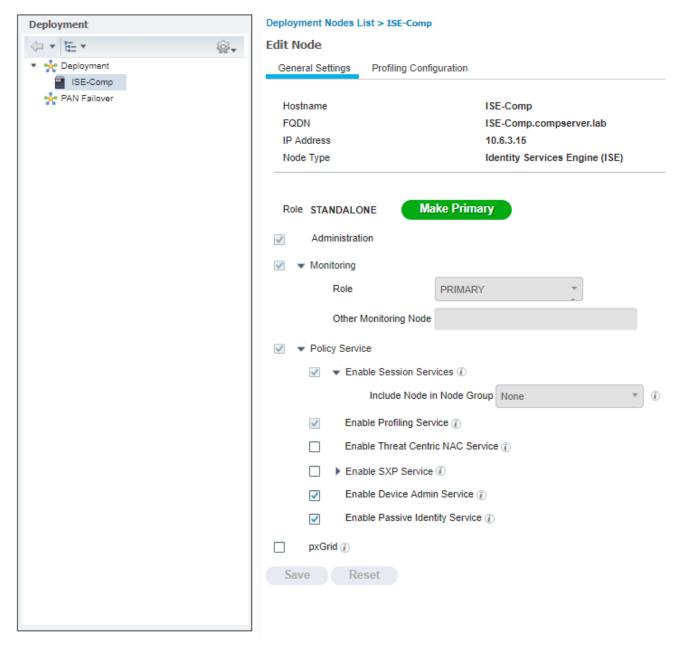


ENABLING TACACS IN CISCO ISE

Description

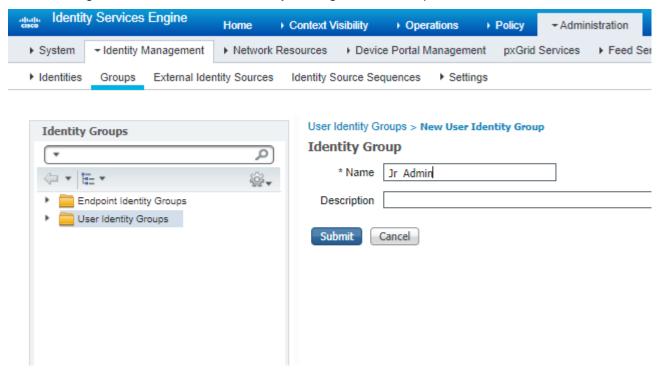
This section will show how to enable the TACACS service within Cisco ISE this section will also go over creating a user and user groups.

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





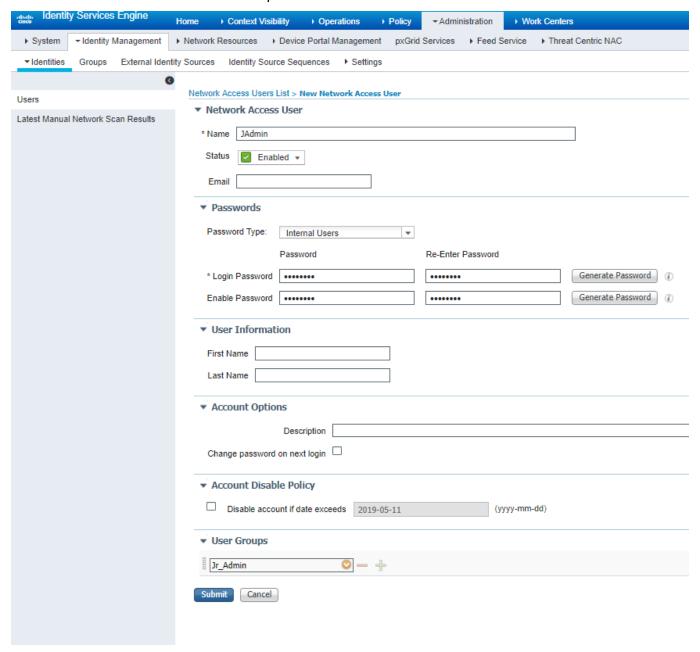
2. Next create a user group within ISE this is to make the policy easier to configure in the future. Navigate to "Administration>Identity management> Groups"





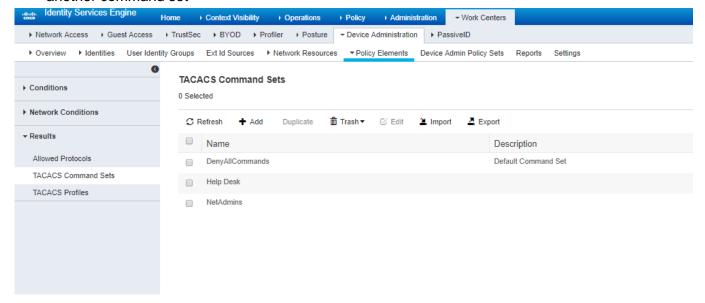
3. Next Create a user Navigate to "Administration> Identity Management> Identities" and Click "+ Add"

Here set the login password and enable password also set the user to the proper group in this case it will be the Jr.Admin Group

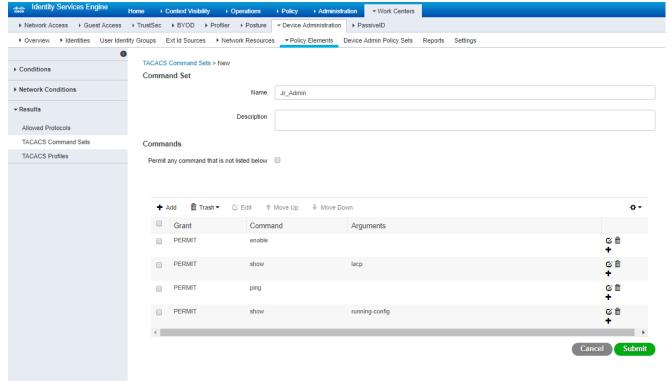




4. Next is to restrict the amount of commands the Jr. Admins can use. Navigate to "Work Centers> Device Administration> Policy Elements" Click Results and "Command sets" Click Add to add another command set

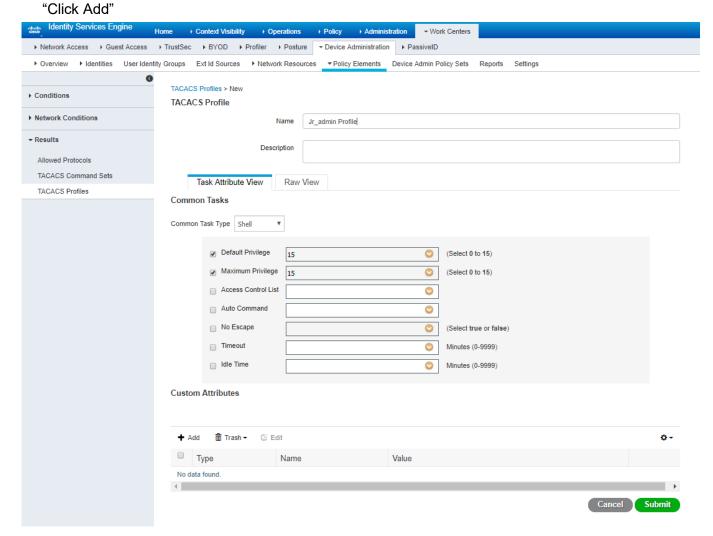


5. All the commands that the Jr. Admin can use will be defined here. A few commands are defined below for example. Click Submit.





6. Next a profile has to be configured. This is to set the privileged level with ArubaOS-Switch it will be set to 15, but based on the command set, it will allow/disallow the user to use certain commands. Navigate to "Work Centers>Device Administration>Policy Elements" "Results >TACACS Profiles"
"Click Add"





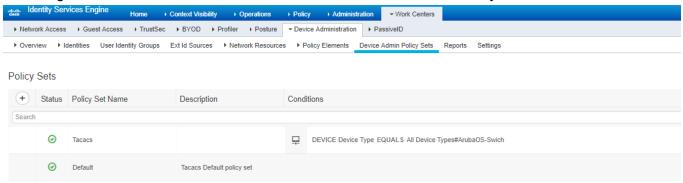
CREATING A TACACS POLICY

Description

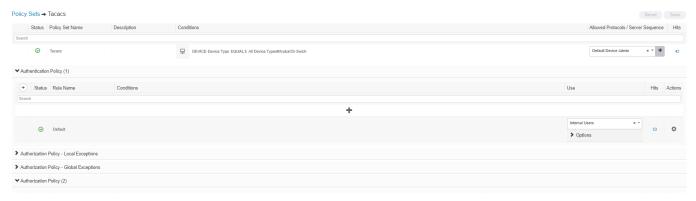
This section will go over how to create a TACACS policy.

1. Create a policy for a TACACS rule, the rule, in this case, is set to match on the devices in the ArubaOS-Switch Group. This is set under the device type when adding a device into ISE.

Navigate to "Work Centers>Device Administration> Device Admin Policy Sets"

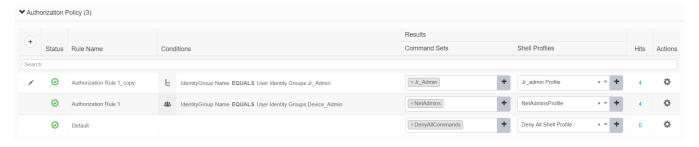


2. Set the authentication mechanism in this case its set to internal users





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 Jr.Admin" that was configured before. The command set result will be the "JrAdmin command set" as well, the profile will be set to the "Jr Admin Profile"

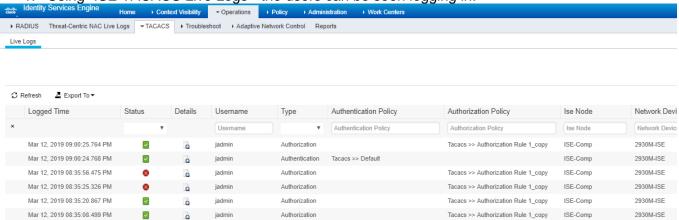






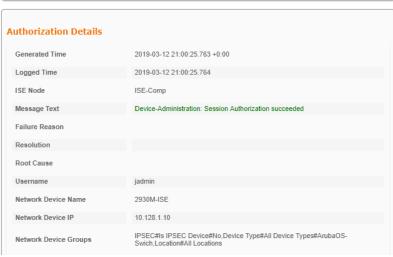
VERIFICATION

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



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







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

```
10.128.1.10 - PuTTY
                                                                           ×
2930M-ISE#
2930M-ISE#
2930M-ISE#
2930M-ISE# ping 10.6.3.12
10.6.3.12 is alive, time = 1 \text{ ms}
2930M-ISE# conf t
Not authorized to run this command
2930M-ISE# page
2930M-ISE# show running-config
Running configuration:
 hpStack WC Configuration Editor; Created on release #WC.16.08.0002
 Ver #14:27.6f.f8.ld.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:04
stacking
  member 1 type "JL323A" mac-address f40343-de4740
  member 1 flexible-module A type JL083A
   exit
hostname "2930M-ISE"
class ipv4 "DNS"
```

3. Doing a "show authentication last-login" will show last login sessions on the switch.

```
10.128.1.10 - PuTTY
                                                                                                                                        2930M-ISE#
2930M-ISE# show authentication last-login
 Username
                          Priv Last Login
                                                          Last Login IP Address
                                                                                                           Fails Last Failed Attempt
                         Oper 2019-03-12 12:08:05 10.6.3.26
Mgr 2019-03-11 14:16:20 10.6.3.26
                                                                                                                   2019-03-12 12:29:45
 Jadmin
 admin
                                                                                                                   2019-03-12 12:30:54
 jadmin
                          Mgr
                               2019-03-12 13:00:32 10.6.3.26
 manager
                          Mgr
                                2019-03-12 12:33:24 10.6.3.26
2019-03-11 14:04:11 10.6.3.26
2019-03-11 14:06:38 10.6.3.26
 netadmin
                          Mgr
                                                                                                                   2019-03-11 14:46:08
 user01
                          Mgr
 user02
                          Mgr
2930M-ISE#
```