

TACACS+ W/ CISCO ISE AND AOS-CX

CONTENTS

TACACS+ W/ Cisco ISE and AOS-CX	1
Requirements.....	1
Overview	1
Adding Devices to Cisco ISE.....	2
Enabling TACACS In Cisco ISE	3
Creating a TACACS Policy.....	7
Verification	8

REQUIREMENTS

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

OVERVIEW

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

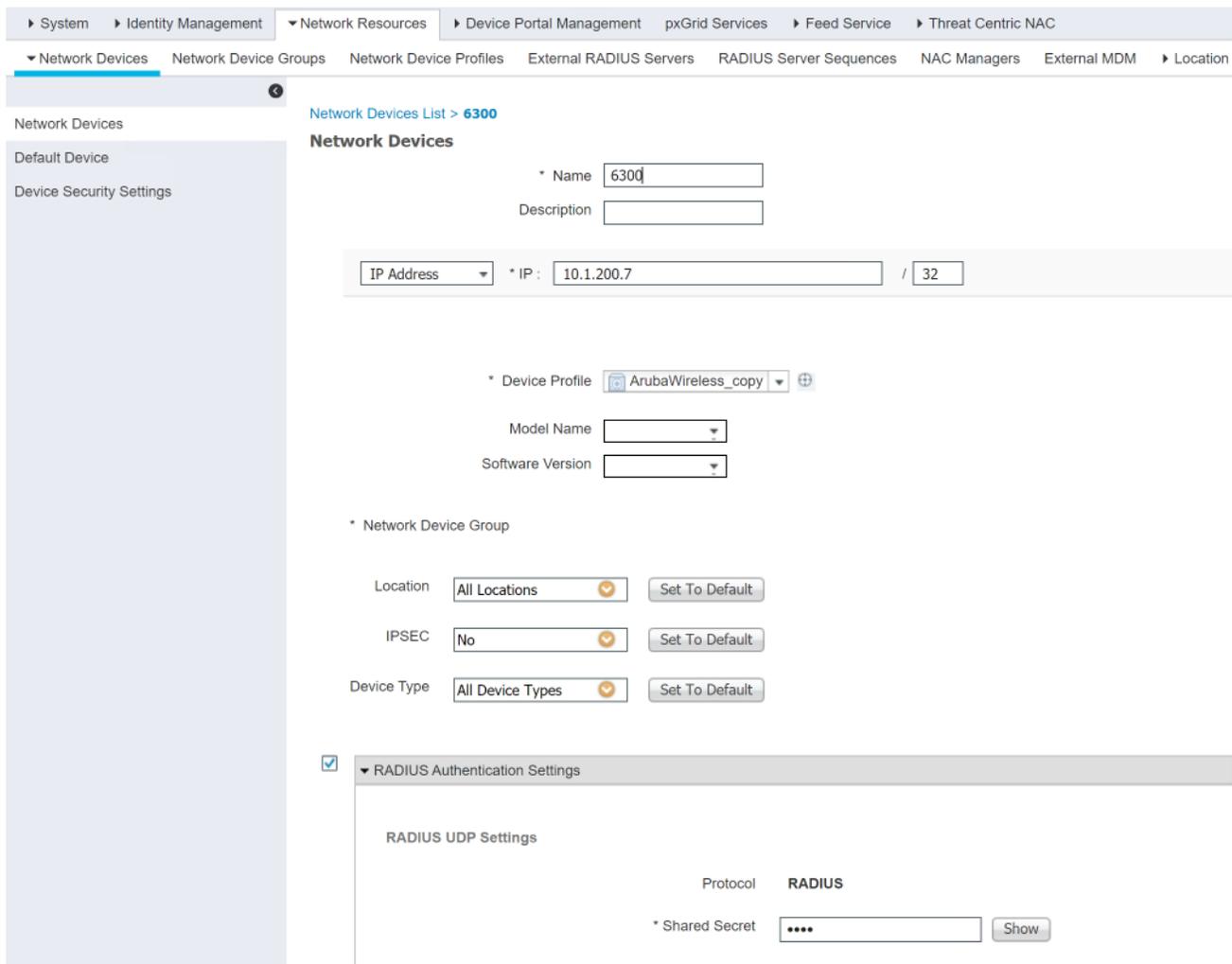
In this scenario, we will create a local user “Joe_admin” Admin TACACS user locally with ISE and restrict the commands so that the “Joe_admin” can use. This document will also show how to verify the user has successfully logged in and can use the authorized commands.

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](#)



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

Network Devices List > 6300

Network Devices

* Name

Description

IP Address /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

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.

The screenshot displays the Cisco ISE web interface for configuring a deployment node. On the left, a navigation pane shows 'Deployment' and 'PAN Failover'. The main content area is titled 'Deployment Nodes List > CISCO-ISE' and 'Edit Node'. It has two tabs: 'General Settings' (selected) and 'Profiling Configuration'. The 'General Settings' tab shows the following configuration:

Hostname	CISCO-ISE
FQDN	CISCO-ISE.aruba.lab
IP Address	10.6.9.31
Node Type	Identity Services Engine (ISE)

Below the table, the 'Role' is set to 'STANDALONE' with a green 'Make Primary' button. A list of services is shown with checkboxes:

- Administration
- Monitoring
 - Role: PRIMARY
 - Other Monitoring Node: [text input]
- Policy Service
 - Enable Session Services
 - Include Node in Node Group: None
 - Enable Profiling Service
 - Enable Threat Centric NAC Service
 - Enable SXP Service
 - Enable Device Admin Service
 - Enable Passive Identity Service
- pxGrid

At the bottom, there are 'Save' and 'Reset' buttons.

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

Users

Latest Manual Network Scan Results

Network Access Users List > **New Network Access User**

▼ Network Access User

* Name

Status Enabled ▼

Email

▼ Passwords

Password Type: ▼

Password

* Login Password ⓘ

Re-Enter Password

Enable Password ⓘ

▼ User Information

First Name

Last Name

▼ Account Options

Description

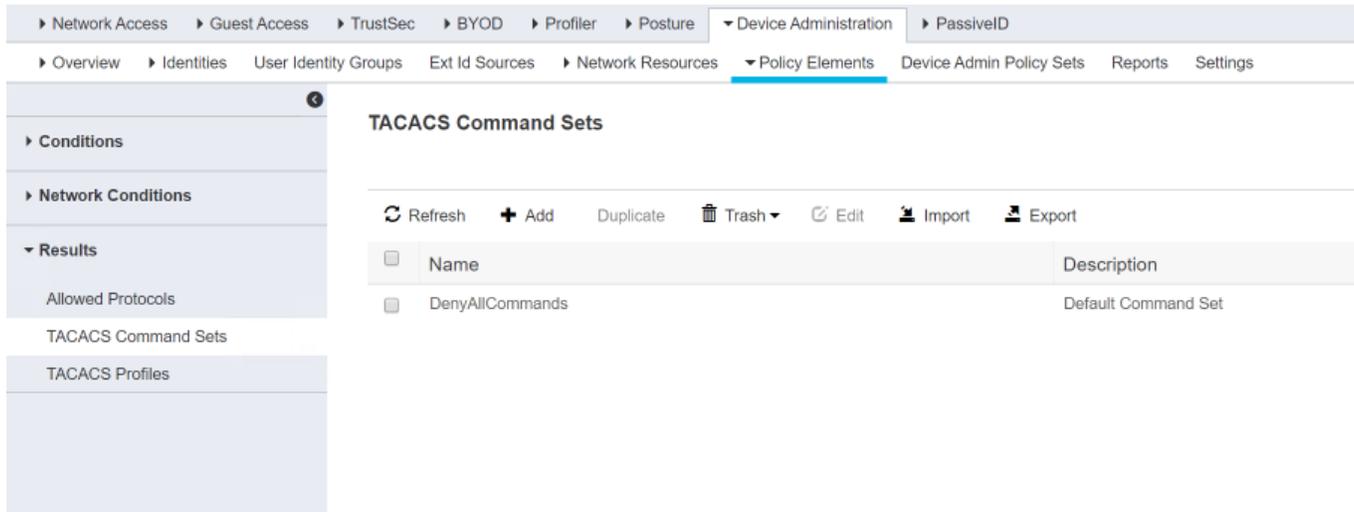
Change password on next login

▼ Account Disable Policy

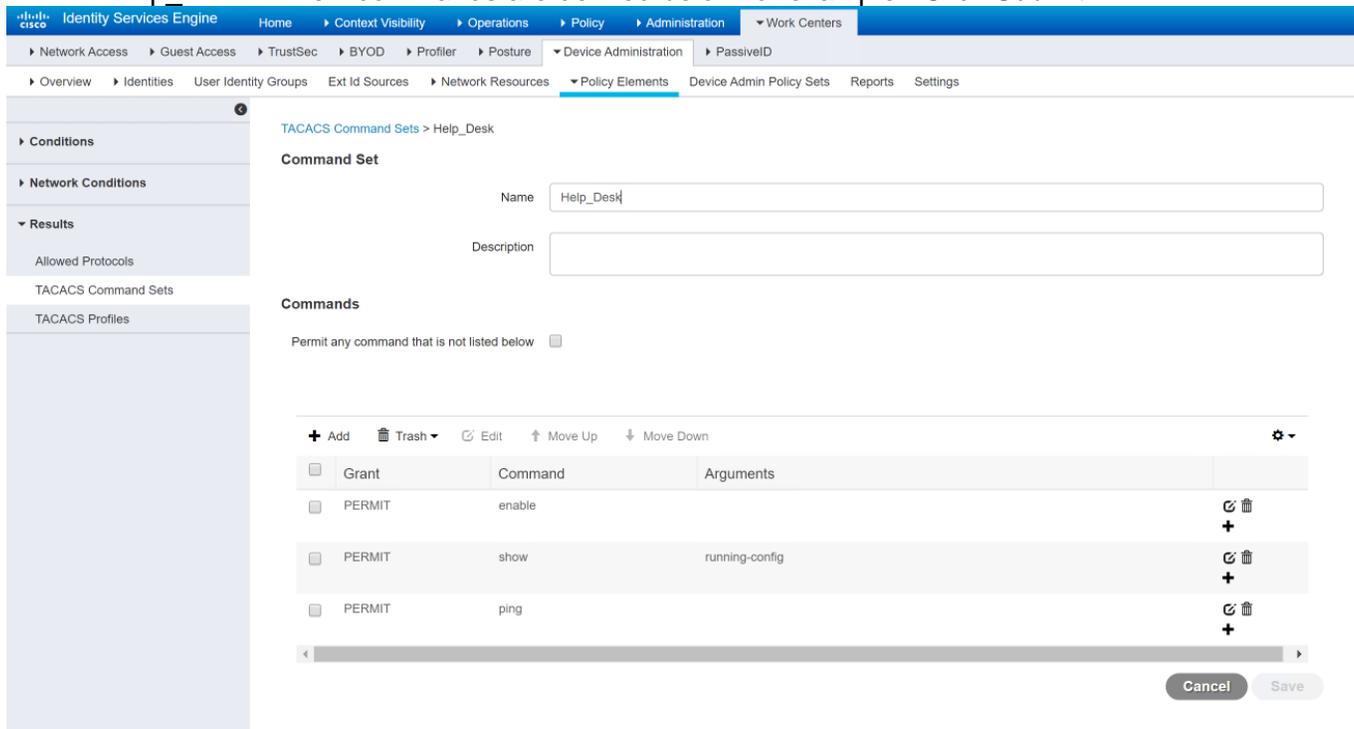
Disable account if date exceeds (yyyy-mm-dd)

▼ User Groups

- 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



- 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.



- 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"

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements > TACACS Profiles > HelpDesk_Profile.

TACACS Profile Configuration:

- Name:** HelpDesk_Profile
- Description:** (Empty text box)

Task Attribute View / Raw View: (Task Attribute View is selected)

Common Tasks:

- Common Task Type: Shell
- Default Privilege:** 15 (Select 0 to 15)
- Maximum Privilege:** 15 (Select 0 to 15)
- Access Control List:** (Empty dropdown)
- Auto Command:** (Empty dropdown)
- No Escape:** (Empty dropdown) (Select true or false)
- Timeout:** (Empty dropdown) Minutes (0-9999)
- Idle Time:** (Empty dropdown) Minutes (0-9999)

Custom Attributes:

Buttons: + Add, Trash, Edit

Type	Name	Value
No data found.		

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”

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
✔	New Policy Set 1		DEVICE Network Device Profile EQUALS ArubaWireless_copy	Default Device Admin
✔	Default	Tacacs Default policy set		Default Device Admin

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

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Authentication Rule 1	DEVICE Network Device Profile EQUALS ArubaWireless_copy	Internal Users	528	Options
✔	Default		All_User_ID_Stores	0	Options

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”

Status	Rule Name	Conditions	Results	Hits	Actions
✔	Local Exceptions Rule 1	IdentityGroup-Name EQUALS User Identity Groups:Employee	Command Sets: Help_Desk; Shell Profiles: HelpDesk_Profile	28	Options

VERIFICATION

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

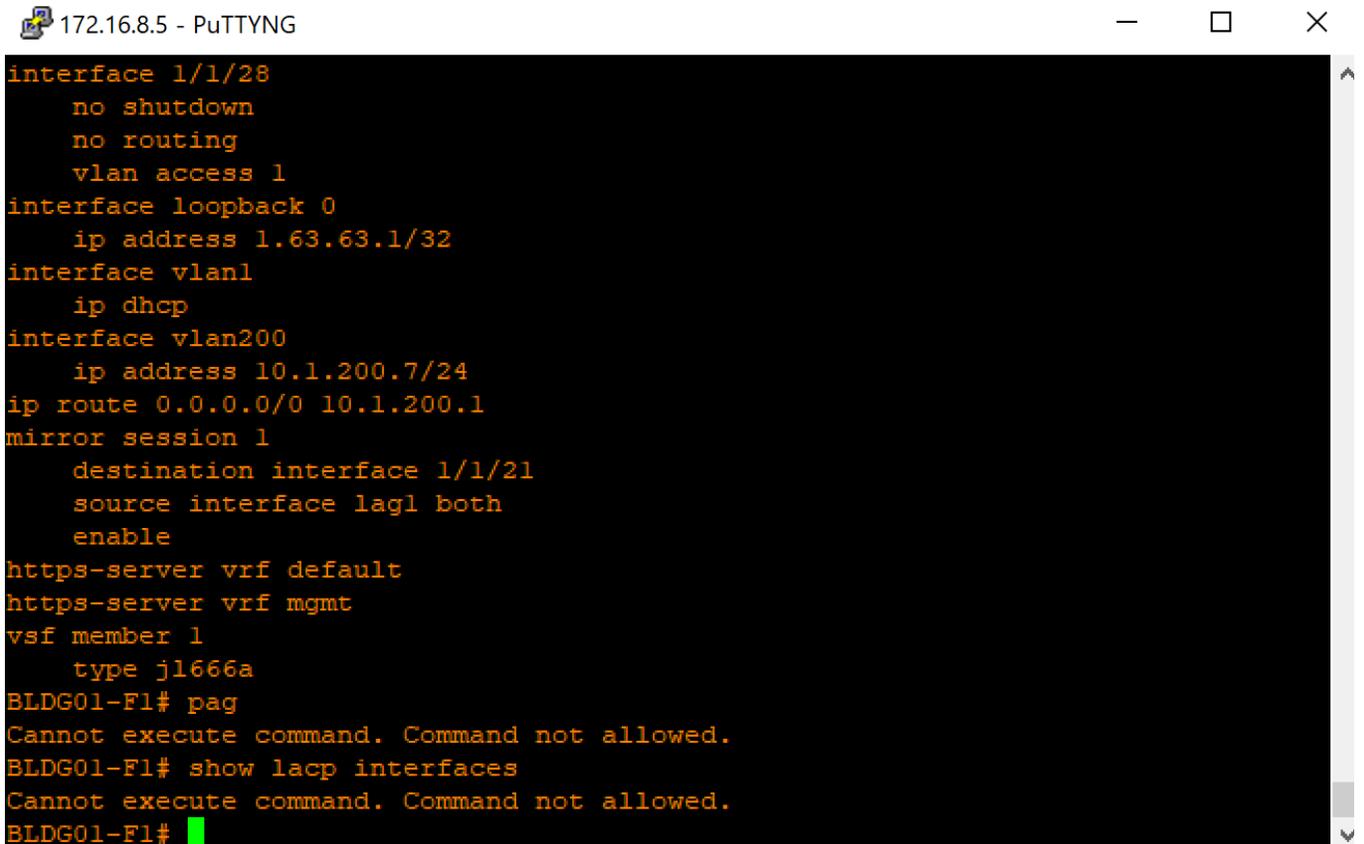
Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node
Feb 25, 2020 11:24:54.953 AM	✗		Joe_Admin	Authorization		New Policy Set 1 >> Local Exception...	CISCO-ISE
Feb 25, 2020 11:24:38.749 AM	✗		Joe_Admin	Authorization		New Policy Set 1 >> Local Exception...	CISCO-ISE
Feb 25, 2020 11:24:26.843 AM	✓		Joe_Admin	Authorization		New Policy Set 1 >> Local Exception...	CISCO-ISE
Feb 25, 2020 09:52:06.457 AM	✓		Joe_Admin	Authorization		New Policy Set 1 >> Local Exception...	CISCO-ISE
Feb 25, 2020 09:51:59.325 AM	✓		Joe_Admin	Authorization		New Policy Set 1 >> Local Exception...	CISCO-ISE
Feb 25, 2020 09:51:59.279 AM	✓		Joe_Admin	Authorization		New Policy Set 1 >> Local Exception...	CISCO-ISE
Feb 25, 2020 09:51:59.242 AM	✓		Joe_Admin	Authentication	New Policy Set 1 >> Authentication R...		CISCO-ISE

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

Session Key	CISCO-ISE/370756711/634
Message Text	Passed-Authentication: Authentication succeeded
Username	Joe_Admin
Authentication Policy	New Policy Set 1 >> Authentication Rule 1
Selected Authorization Profile	HelpDesk_Profile

Authentication Details	
Generated Time	2020-02-25 09:51:59.233000 -08:00
Logged Time	2020-02-25 09:51:59.242
Epoch Time (sec)	1582653119
ISE Node	CISCO-ISE
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	Joe_Admin
Network Device Name	6300
Network Device IP	10.1.200.7
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	ssh

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



172.16.8.5 - PuTTYNG

```
interface 1/1/28
  no shutdown
  no routing
  vlan access 1
interface loopback 0
  ip address 1.63.63.1/32
interface vlan1
  ip dhcp
interface vlan200
  ip address 10.1.200.7/24
ip route 0.0.0.0/0 10.1.200.1
mirror session 1
  destination interface 1/1/21
  source interface lag1 both
  enable
https-server vrf default
https-server vrf mgmt
vsf member 1
  type j1666a
BLDG01-F1# pag
Cannot execute command. Command not allowed.
BLDG01-F1# show lacp interfaces
Cannot execute command. Command not allowed.
BLDG01-F1#
```