

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](#)

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes: System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NAC. The left sidebar shows: Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, and Location. The main content area is titled 'Network Devices' and shows a list of 6300 devices. The 'Add Device' form is displayed with the following fields:

- Name:** 6300
- Description:** (empty)
- IP Address:** 10.1.200.7 / 32
- Device Profile:** ArubaWireless_copy
- Model Name:** (empty)
- Software Version:** (empty)
- Network Device Group:** (empty)
- Location:** All Locations (Set To Default)
- IPSEC:** No (Set To Default)
- Device Type:** All Device Types (Set To Default)
- RADIUS Authentication Settings:** (checked)
 - RADIUS UDP Settings:**
 - Protocol:** RADIUS
 - Shared Secret:** (masked with dots) (Show)

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.

Deployment

Deployment Nodes List > CISCO-ISE

Edit Node

General Settings Profiling Configuration

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

Role: STANDALONE Make Primary

☒ Administration

☒ Monitoring

Role: PRIMARY

Other Monitoring Node

☒ 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

Save Reset

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

Re-Enter Password

* Login Password

Generate Password

Enable Password

Generate 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

Employee

Submit

Cancel

4

- 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

The screenshot shows the Aruba ISE web interface. The breadcrumb navigation is: Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID. The left sidebar shows a tree view with 'Results' expanded, containing 'Allowed Protocols', 'TACACS Command Sets', and 'TACACS Profiles'. The main content area is titled 'TACACS Command Sets' and includes a toolbar with 'Refresh', '+ Add', 'Duplicate', 'Trash', 'Edit', 'Import', and 'Export'. Below the toolbar is a table with two columns: 'Name' and 'Description'. The table contains one entry: 'DenyAllCommands' with the description 'Default 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.

The screenshot shows the 'Add Command Set' form in the Aruba ISE web interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > PassiveID. The left sidebar is the same as the previous screenshot. The main content area is titled 'TACACS Command Sets > Help_Desk'. It contains a 'Command Set' section with a 'Name' field containing 'Help_Desk' and an empty 'Description' field. Below this is a 'Commands' section with a checkbox 'Permit any command that is not listed below' which is unchecked. A table lists commands to be added, with columns for 'Grant', 'Command', and 'Arguments'. The table contains three entries: 'PERMIT enable', 'PERMIT show running-config', and 'PERMIT ping'. Each entry has a trash icon and a plus icon to its right. At the bottom right are 'Cancel' and 'Save' buttons.

- 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”

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

TACACS Profiles > HelpDesk_Profile

TACACS Profile

Name: HelpDesk_Profile

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

☒ Default Privilege: 15 (Select 0 to 15)
☒ Maximum Privilege: 15 (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

+ 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”

The screenshot shows the 'Device Admin Policy Sets' page in the ISE interface. It features a table with the following columns: Status, Policy Set Name, Description, Conditions, and Allowed Protocols / Server Sequence. There are two rows: 'New Policy Set 1' and 'Default'. The 'New Policy Set 1' row has a condition 'DEVICE Network Device Profile EQUALS ArubaWireless_copy' and 'Default Device Admin' for allowed protocols. The 'Default' row has a description 'Tacacs Default policy set' and 'Default Device Admin' for allowed protocols.

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

The screenshot shows the 'Authentication Policy' configuration for 'New Policy Set 1'. It includes a table with columns: Status, Rule Name, Conditions, Use, Hits, and Actions. There are two rows: 'Authentication Rule 1' and 'Default'. The 'Authentication Rule 1' row has a condition 'DEVICE Network Device Profile EQUALS ArubaWireless_copy', is set to 'Internal Users', and has 528 hits. The 'Default' row is set to 'All_User_ID_Stores' and has 0 hits.

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”

The screenshot shows the 'Authorization Policy - Local Exceptions' configuration for 'Local Exceptions Rule 1'. It includes a table with columns: Status, Rule Name, Conditions, Results (Command Sets, Shell Profiles), Hits, and Actions. The 'Local Exceptions Rule 1' row has a condition 'IdentityGroup-Name EQUALS User Identity Groups:Employee', a command set 'Help_Desk', a shell profile 'HelpDesk_Profile', and 28 hits.

VERIFICATION

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

Cisco Identity Services Engine								
Home Context Visibility Operations Policy Administration Work Centers								
RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports								
Live Logs								
Refresh Never Show								
Refresh Export To								
Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	
x			Identity		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#
```