

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	5
Creating a TACACS Policy.....	10
Verification	12

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.”

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded, showing 'System', 'Identity Management', and 'Network Resources'. Under 'Network Resources', 'Network Devices' is selected. The main content area shows the 'Network Devices' page with a table of existing devices. The table has columns for Name, IP/Mask, Profile Name, Location, and Type. One device is listed: '2930M-ISE' with IP/Mask '10.128.1.10/32', Profile Name 'HPWired_copy', Location 'All Locations', and Type 'All Device Types'. Action buttons for Edit, Add, Duplicate, Import, Export, Generate PAC, and Delete are visible above the table.

Name	IP/Mask	Profile Name	Location	Type
<input type="checkbox"/> 2930M-ISE	10.128.1.10/32	HPWired_copy	All Locations	All Device Types

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.

Network Devices List > 2930M-ISE

Network Devices

* Name

Description

IP Address /

i IPv6 is supported only for TACACS. At least one IPv4 must be defined when RADIUS is selected

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

▶ RADIUS Authentication Settings

▼ TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

- Legacy Cisco Device
- TACACS Draft Compliance Single Connect Support

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.

Deployment

- Deployment
 - ISE-Comp
 - PAN Failover

[Deployment Nodes List > ISE-Comp](#)

Edit Node

General Settings | Profiling Configuration

Hostname	ISE-Comp
FQDN	ISE-Comp.compserver.lab
IP Address	10.6.3.15
Node Type	Identity Services Engine (ISE)

Role: STANDALONE **Make Primary**

- Administration
- Monitoring
 - Role: PRIMARY
 - Other Monitoring Node: [Empty]
- 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 group within ISE this is to make the policy easier to configure in the future. Navigate to “Administration>Identity management> Groups”

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', and 'Administration'. The 'Administration' menu is expanded to show 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', and 'Feed Services'. The 'Identity Management' menu is further expanded to show 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Groups' menu item is selected.

The main content area is titled 'User Identity Groups > New User Identity Group'. It features a search bar and a navigation pane on the left with 'Endpoint Identity Groups' and 'User Identity Groups' (selected). The main form area is titled 'Identity Group' and contains the following fields and buttons:

- * Name:
- Description:
- Submit button
- Cancel button

- 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

The screenshot shows the Aruba Identity Services Engine (ISE) web interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Identity Management > Identities > New Network Access User. The page is titled "Network Access Users List > New Network Access User".

Network Access User

- * Name: JAdmin
- Status: Enabled
- Email: [Empty field]

Passwords

- Password Type: Internal Users
- * Login Password: [Masked] [Generate Password]
- Re-Enter Password: [Masked] [Generate Password]
- Enable Password: [Masked] [Generate Password]

User Information

- First Name: [Empty field]
- Last Name: [Empty field]

Account Options

- Description: [Empty field]
- Change password on next login:

Account Disable Policy

- Disable account if date exceeds: 2019-05-11 (yyyy-mm-dd)

User Groups

- Jr_Admin [Dropdown menu]

Buttons: Submit, Cancel

- 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

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements

TACACS Command Sets

0 Selected

Refresh Add Duplicate Trash Edit Import Export

Name	Description
DenyAllCommands	Default Command Set
Help Desk	
NetAdmins	

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

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements

TACACS Command Sets > New Command Set

Name: Jr_Admin

Description:

Commands

Permit any command that is not listed below

Grant	Command	Arguments
PERMIT	enable	
PERMIT	show	lacp
PERMIT	ping	
PERMIT	show	running-config

Cancel Submit

- 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”

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassivID

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings

TACACS Profiles > New

TACACS Profile

Name Jr_admin 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.		

Cancel Submit

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”

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

Policy Sets

+ Status	Policy Set Name	Description	Conditions
On	Tacacs		DEVICE Device Type EQUALS All Device Types#ArubaOS-Switch
On	Default	Tacacs Default policy set	

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

Policy Sets - Tacacs

Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
On	Tacacs		DEVICE Device Type EQUALS All Device Types#ArubaOS-Switch	Default Device Admin	42

Authentication Policy (1)

+ Status	Rule Name	Conditions	Use	Hits	Actions
On	Default		Internal Users	53	Options

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (2)

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”

Authorization Policy (3)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Command Sets	Shell Profiles		
Search							
		Authorization Rule 1_copy	IdentityGroup Name EQUALS User Identity Groups:Jr_Admin	Jr_Admin	Jr_admin Profile	4	
		Authorization Rule 1	IdentityGroup Name EQUALS User Identity Groups:Device_Admin	NetAdmins	NetAdminsProfile	4	
		Default		DenyAllCommands	Deny All Shell Profile	0	

Reset Save

VERIFICATION

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

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 Export To

Logged Time	Status	Details	Username	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devi
Mar 12, 2019 09:00:25.764 PM	✓		jadmin	Authorization		Tacacs >> Authorization Rule 1_copy	ISE-Comp	2930M-ISE
Mar 12, 2019 09:00:24.768 PM	✓		jadmin	Authentication	Tacacs >> Default		ISE-Comp	2930M-ISE
Mar 12, 2019 08:35:56.475 PM	✗		jadmin	Authorization		Tacacs >> Authorization Rule 1_copy	ISE-Comp	2930M-ISE
Mar 12, 2019 08:35:25.326 PM	✗		jadmin	Authorization		Tacacs >> Authorization Rule 1_copy	ISE-Comp	2930M-ISE
Mar 12, 2019 08:35:20.867 PM	✓		jadmin	Authorization		Tacacs >> Authorization Rule 1_copy	ISE-Comp	2930M-ISE
Mar 12, 2019 08:35:08.499 PM	✓		jadmin	Authorization		Tacacs >> Authorization Rule 1_copy	ISE-Comp	2930M-ISE

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

Overview

Request Type	Authorization
Status	Pass
Session Key	ISE-Comp/341383157/379
Message Text	Device-Administration: Session Authorization succeeded
Username	jadmin
Authorization Policy	Tacacs >> Authorization Rule 1_copy
Shell Profile	Jr_admin Profile
Matched Command Set	
Command From Device	

Authorization Details

Generated Time	2019-03-12 21:00:25.763 +0:00
Logged Time	2019-03-12 21:00:25.764
ISE Node	ISE-Comp
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	jadmin
Network Device Name	2930M-ISE
Network Device IP	10.128.1.10
Network Device Groups	IPSEC#Is IPSEC Device#No.Device Type#All Device Types#ArubaOS-Switch.Location#All Locations

- 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 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"
  
```

- Doing a “show authentication last-login” will show last login sessions on the switch.

```

10.128.1.10 - PuTTY
2930M-ISE#
2930M-ISE#
2930M-ISE#
2930M-ISE#
2930M-ISE#
2930M-ISE#
2930M-ISE#
2930M-ISE#
2930M-ISE#
2930M-ISE#
2930M-ISE#
2930M-ISE#
2930M-ISE#
2930M-ISE#
2930M-ISE# show authentication last-login

Username           Priv  Last Login           Last Login IP Address  Fails  Last Failed Attempt
-----
Jadmin             Oper  2019-03-12 12:08:05  10.6.3.26              1      2019-03-12 12:29:45
admin              Mgr   2019-03-11 14:16:20  10.6.3.26              3      2019-03-12 12:30:54
jadmin             Mgr   2019-03-12 13:00:32  10.6.3.26              0
manager           Mgr   2019-03-11 14:14:17  10.6.3.26              0
netadmin          Mgr   2019-03-12 12:33:24  10.6.3.26              0
user01            Mgr   2019-03-11 14:04:11  10.6.3.26              4      2019-03-11 14:46:08
user02            Mgr   2019-03-11 14:06:38  10.6.3.26              0
2930M-ISE#
  
```