

**This Document is best viewed in Web Layout**

## **Setting up Cisco-ISE for RADIUS Authentication to Support Cambium cnPilot Products.**

### **Setting up Cisco ISE for RADIUS Services**

#### **Overview**

This document presents basic configuration of Cisco ISE 2.4.0.357 as RADIUS server.

#### **Server Information**

Username: **admin**  
Host: **cnmaestrositise**  
Personas: **Administration, Monitoring, Policy Service (SESSION,PROFILER,DEVICE ADMIN)**  
Role: **STANDALONE**  
System time: **May 21 2019 08:18:51 AM UTC**  
FIPS mode: **Disabled**  
Version: **2.4.0.357**  
Patch Information: **none**

OK

#### **Pre-requisites**

1. Cisco ISE Installed on VM
2. Latest Chrome/Firefox browser

#### **Configuration:**

The steps below configure the Cisco-ISE server for RADIUS authentication to be used by Cambium products.

#### **Step1: Adding new RADIUS Vendor**

1. Navigate to Policy > Policy Elements > Dictionaries > System > Radius > RADIUS Vendors

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Dictionaries

Search

← ↗ ⚙

- ▶ NMAP
- ▶ NMAPExtension
- ▶ Normalised Radius
- ▶ PassiveID
- ▶ Posture
- ▶ PROFILER
- ▶ Radius
  - ▶ IETF
  - ▶ RADIUS Vendors
    - ▶ Airespace
    - ▶ Alcatel-Lucent
    - ▶ Aruba
    - ▶ Brocade
    - ▶ CambiumNetworks
    - ▶ Cisco
    - ▶ Cisco-BBSM
    - ▶ Cisco-VPN3000
    - ▶ H3C
    - ▶ HP
    - ▶ Juniper

**RADIUS Vendors**

Edit Add Delete Import Export

<input type="checkbox"/>	Name	Vendor ID	Description
<input type="checkbox"/>	Airespace	14179	Dictionary for Vendor Airespace
<input type="checkbox"/>	Alcatel-Lucent	800	Dictionary for Vendor Alcatel-Lucent
<input type="checkbox"/>	Aruba	14823	Dictionary for Vendor Aruba
<input type="checkbox"/>	Brocade	1588	Dictionary for Vendor Brocade
<input type="checkbox"/>	CambiumNetworks	17713	Dictionary for vendor CambiumNetworks
<input type="checkbox"/>	Cisco	9	Dictionary for Vendor Cisco
<input type="checkbox"/>	Cisco-BBSM	5263	Dictionary for Vendor Cisco-BBSM
<input type="checkbox"/>	Cisco-VPN3000	3076	Dictionary for Vendor Cisco-VPN3000
<input type="checkbox"/>	H3C	25506	Dictionary for Vendor H3C
<input type="checkbox"/>	HP	11	Dictionary for Vendor HP
<input type="checkbox"/>	Juniper	2636	Dictionary for Vendor Juniper
<input type="checkbox"/>	Microsoft	311	Dictionary for Vendor Microsoft
<input type="checkbox"/>	Motorola-Symbol	388	Dictionary for Vendor Motorola-Symbol
<input type="checkbox"/>	Ruckus	25053	Dictionary for Vendor Ruckus
<input type="checkbox"/>	WISPr	14122	Dictionary for Vendor WISPr
<input type="checkbox"/>	moto	161	Motorola vendor for cambium

- Click Add and provide proper details in the required fields, then click on submit.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Dictionaries

Search

← ↗ ⚙

- ▶ NMAP
- ▶ NMAPExtension
- ▶ Normalised Radius
- ▶ PassiveID
- ▶ Posture
- ▶ PROFILER
- ▶ Radius
  - ▶ IETF
  - ▶ RADIUS Vendors
    - ▶ Airespace
    - ▶ Alcatel-Lucent
    - ▶ Aruba
    - ▶ Brocade
    - ▶ CambiumNetworks
    - ▶ Cisco
    - ▶ Cisco-BBSM
    - ▶ Cisco-VPN3000
    - ▶ H3C
    - ▶ HP
    - ▶ Juniper

**RADIUS Vendors List > New RADIUS Vendor**

\* Dictionary Name

Description

\* Vendor ID

Vendor Attribute Type Field Length

Vendor Attribute Size Field Length

Submit Cancel

## Step2: Adding Network Device Profiles

- Navigate to Administration > Network Resources > Network Device Profiles > Click +Add

Network Device Profiles

Edit
Add
Duplicate
Import
Cisco Communities Import
Export Selected
Delete Selected

<input type="checkbox"/>	Name	Description	Vendor
<input type="checkbox"/>	AlcatelWired	Profile for Alcatel switches	Alcatel
<input type="checkbox"/>	ArubaWireless	Profile for Aruba wireless network access devices	Aruba
<input type="checkbox"/>	BrocadeWired	Profile for Brocade switches	Brocade
<input type="checkbox"/>	Anand_SA_Test	This is created for testing purpose	Cisco
<input type="checkbox"/>	Cisco	Generic profile for Cisco network access devices	Cisco
<input type="checkbox"/>	HPWired	Profile for HP switches	HP
<input type="checkbox"/>	HPWired_SNMP_CoA	Profile for HP switches with no RADIUS CoA	HP
<input type="checkbox"/>	HPWireless	Profile for HP wireless network access devices	HP
<input type="checkbox"/>	MotorolaWireless	Profile for Motorola wireless network access devices	Motorola
<input type="checkbox"/>	Cambium-PMP		Other
<input type="checkbox"/>	CambiumNetworks	Profile for Cambium device	Other
<input type="checkbox"/>	Cambium_TACplus		Other
<input type="checkbox"/>	RuckusWireless	Profile for Ruckus wireless network access devices	Ruckus

2. Provide valid details and submit


[Network Device Profile List](#) > [New Network Device Profile](#)

## Network Device Profile

Submit

\* Name

Description

Icon 

Vendor

### Supported Protocols

RADIUS ☐

TACACS+ ☐

TrustSec ☐

RADIUS Dictionaries

### Templates

[Expand All](#) / [Collapse All](#)

[Authentication/Authorization](#)

[Permissions](#)

[Change of Authorization \(CoA\)](#)

[Redirect](#)

[Advanced](#)

### Step3: Adding Network Device

1. Navigate to Administration > Network Resources > Network Devices

**Identity Services Engine** Home Context Visibility Operations Policy Administration Work Centers

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

**Network Devices**

Default Device  
Device Security Settings

**Network Devices**

Edit Add Duplicate Import Export Generate PAC Delete

	Name	IP/Mask	Profile Name	Location	Type
<input type="checkbox"/>	PMP-AP	10.110.250.1/32	Cambium-PMP	All Locations	All Device
<input type="checkbox"/>	ankit	10.23.41.1/24	CambiumNetworks	All Locations	All Device
<input type="checkbox"/>	ankit1	172.26.120.21...	CambiumNetworks	All Locations	All Device
<input type="checkbox"/>	cnMaestro	10.110.209.1/24	CambiumNetworks	All Locations	All Device
<input type="checkbox"/>	cnMaestro_TAC	192.168.1.0/16	Cambium_TACplus	All Locations	All Device

2. Click +Add ,
3. Provide Name, description, IP Address/Range,
4. Select the newly created device profile. (in the previous step)
5. Let Network device group values be default.
6. Enable Radius Authentication Settings and configure Shared secret.
7. Save

Identity Services Engine

Home

Context Visibility

Operations

Policy

Administration

Work Centers

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

Third Party Vendors

MDM

Network Devices

Default Device

Device Security Settings

Network Devices List > New Network Device

Network Devices

\* Name

solution\_team

Description

Solution\_team\_Networ

IP Address

\* IP : 10.110.200.0

/ 24

\* Device Profile

CambiumNetworks

Model Name

Software Version

\* Network Device Group

Location

All Locations

Set To Default

IPSEC

Is IPSEC Device

Set To Default

Device Type

All Device Types

Set To Default

☒ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

RADIUS

\* Shared Secret

.....

Show

Use Second Shared Secret

☐

Show

CoA Port

Set To Default

RADIUS DTLS Settings

DTLS Required

☐

Shared Secret

radius/dtls

CoA Port

Set To Default

Issuer CA of ISE Certificates for CoA

Select if required (optional)

DNS Name

General Settings

Enable KeyWrap

☐

\* Key Encryption Key

Show

\* Message Authenticator Code Key

Show

Key Input Format

☒ ASCII ☐ HEXADECIMAL

☐ TACACS Authentication Settings

☐ SNMP Settings

☐ Advanced TrustSec Settings

Submit

Cancel

### Step 4: Creating User Identities

1. Navigate to Identity Management > Identities >

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' tab is active, and the 'Identities' sub-tab is selected. The main content area is titled 'Network Access Users' and contains a table of users. The table has columns for Status, Name, Description, First Name, Last Name, and Email. The 'Status' column shows a checkbox and a status label (Enabled or Disabled). The 'Name' column shows a user icon and the user name. The 'Description' column shows the user's role or description. The 'First Name' and 'Last Name' columns show the user's name components. The 'Email' column shows the user's email address.

Status	Name	Description	First Name	Last Name	Email
<input type="checkbox"/> Enabled	gayatri		super	user	
<input type="checkbox"/> Enabled	helpdesk		monitor	user	
<input type="checkbox"/> Disabled	moniuser				
<input type="checkbox"/> Enabled	prashanth		ope	user	
<input type="checkbox"/> Disabled	ptpise				
<input type="checkbox"/> Disabled	ptpise1				
<input type="checkbox"/> Disabled	ptpise2				
<input type="checkbox"/> Enabled	raghav		super	user	
<input type="checkbox"/> Disabled	saikumar				
<input type="checkbox"/> Disabled	superuser				
<input type="checkbox"/> Disabled	testpmp				
<input type="checkbox"/> Disabled	user1				
<input type="checkbox"/> Disabled	user4				
<input type="checkbox"/> Enabled	vinod		admin	user	

2. Click + Add and fill the details as mentioned below
3. Name: Name of the user (need to be unique)
4. Status: Enabled by default
5. Email: Email address of the user (optional)
6. Login Password: Password as per password policy
7. User Custom Attributes : Assign a role for the user
8. Click submit

**Identity Services Engine** Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

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

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 Custom Attributes**

\* Role =

**User Groups**

### Step 5: Selection of Authentication Protocols

1. Navigate to Policy > Policy Elements > Results
2. Navigate to Authentication > Allowed Protocols



### Allowed Protocols

► Authorization

- ▶ Profiling

- ▶ Posture

► Client Provisioning

[Allowed Protocols Services List](#) > **New Allowed Protocols Service**

### Allowed Protocols

Name	solution team network access
------	------------------------------

Description	This Access Policy is created for Testing
-------------	-------------------------------------------

▼ Allowed Protocols

## Authentication Bypass

☒ Process Host Lookup ⓘ

## Authentication Protocols

☒ Allow PAP/ASCII☐ Allow CHAP☐ Allow MS-CHAPv1☐ Allow MS-CHAPv2☒ Allow EAP-MD5☒ Allow EAP-TLS☐ Allow LEAP

▼ ☒ Allow PEAP

### PEAP Inner Methods

☒ Allow EAP-MS-CHAPv2

☒ Allow Password Change Retries  (Valid Range 0 to 3)

☐ Allow EAP-GTC

☐ Allow Password Change Retries  (Valid Range 0 to 3)

☒ Allow EAP-TLS

☐ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

☐ Require cryptobinding TLV ⓘ☐ Allow PEAPv0 only for legacy clients

☒ Allow EAP-FAST

### EAP-FAST Inner Methods

☒ Allow EAP-MS-CHAPv2

☒ Allow Password Change Retries  (Valid Range 0 to 3)

☒ Allow EAP-GTC

☒ Allow Password Change Retries  (Valid Range 0 to 3)

☒ Allow EAP-TLS

☐ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

☒ Use PACs ☐ Don't Use PACs

Tunnel PAC Time To Live

Proactive PAC update will occur after 10 % of PAC Time To Live has expired

☐ Allow Anonymous In-Band PAC Provisioning

113

### **Step 6: Creation of Authorization Profiles**

1. Navigate to Policy > Policy Elements > Results
2. Navigate to Authorization > Authorization Profiles and click + Add
3. Name: Provide valid name
4. Access Type: ACCESS ACCEPT
5. Network Device Profile: Select the profile you created for Radius
6. Click on Submit

Policy Sets

Profiling

Posture

Client Provisioning

▼ Policy Elements

Dictionarys

▸ Conditions

▼ Results

▸ Authentication

▼ Authorization

Authorization Profiles

Downloadable ACLs

▸ Profiling

▸ Posture

▸ Client Provisioning

Authorization Profiles > **New Authorization Profile**

**Authorization Profile**

\* Name

Solution\_Auth\_profile

Description

\* Access Type

ACCESS\_ACCEPT

Network Device Profile

Anand\_SA\_Test

Service Template

Track Movement

Passive Identity Tracking

▼ Common Tasks

DAACL Name

ACL

Security Group

VLAN

▼ Advanced Attributes Settings

Select an item

=

▼ Attributes Details

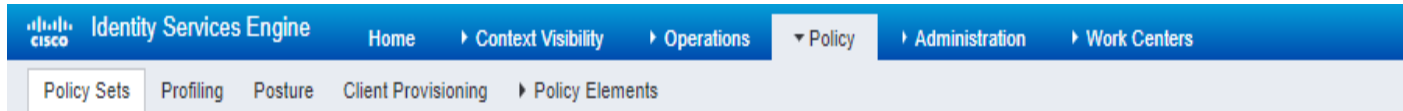
Access Type = ACCESS\_ACCEPT

Submit

Cancel

### Step7: Creation of Policy Sets

1. Navigate to Policy > Policy Sets
2. Click on + symbol and Add the rules
3. Select Allowed protocols as “solution\_team\_network\_access”



#### Policy Sets

	Status	Policy Set Name	Description	Conditions
<input type="text" value="Search"/>				
		Solution_Team_Policy		
		New Policy Set 2		RADIUS-cnMaestro
		New Policy Set 1		Cambium
		Default	Default policy set	

4. Click on + symbol and select the conditions studio, User can select existing rules from conditions studio or can create a new one and save
5. Click Editor to add an attribute and add a rule which equals to Network device profile, so that requests coming from particular device IP ranges will be hitting to this policy.

## Conditions Studio

### Library

Search by Name



	Cambium	
	Catalyst_Switch_Local_Web_Authentic ation	
	RADIUS-cnMaestro	
	Switch_Local_Web_Authentication	
	Switch_Web_Authentication	
	Switch_Web_Authentication_Cambium Networks	
	Wired_802.1X	
	Wired_MAB	
	Wireless_802.1X	
	Wireless_Access	
	Wireless_MAB	
	WLC_Web_Authentication	

### Editor

DEVICE: Network Device Profile




Equals

Anand\_

Set to 'Is not'



6. Select the new policy and click on Authentication policy and use internal users.
7. Select the appropriate Authorization policy
8. Save the policy.


**Identity Services Engine**


[Home](#)
[Context Visibility](#)
[Operations](#)
[Policy](#)
[Administration](#)
[Work Centers](#)

[Policy Sets](#)
[Profiling](#)
[Posture](#)
[Client Provisioning](#)
[Policy Elements](#)

## Policy Sets

+	Status	Policy Set Name	Description	Conditions
Search				
		Solution_Team_Ploicy		DEVICE-Network Device Profile EQUALS Anand_SA_Test
		New Policy Set 2		RADIUS-cnMaestro
		New Policy Set 1		Cambium
		Default	Default policy set	

Policy Sets
 ➔
 Solution\_Team\_Ploicy

	Status	Policy Set Name	Description	Conditions
Search				
	✔	Solution_Team_Ploicy		<div>                      DEVICE: Network Device Profile EQUALS Anand_SA_Test                 </div>

▼ Authentication Policy (1)

+	Status	Rule Name	Conditions
Search			
	✔	Default	

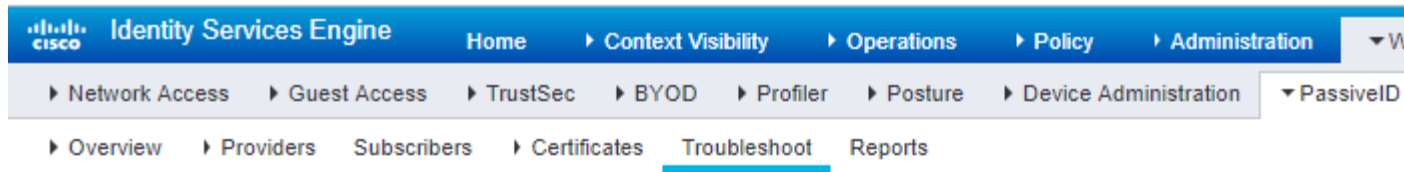
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions

▼ Authorization Policy (1)

+	Status	Rule Name	Conditions
Search			
	✔	Default	


**Step 8: Troubleshooting**

1. Navigate to Work Centers > Passive ID > Troubleshoot
2. Start TCP dump before client connects to RADIUS server.
3. Stop TCP dump once client disconnects and download the file.
4. Wireshark or any other sniffers can be used to analyse the dump.



## TCP Dump

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

Status  Stopped [Start](#)

Host Name

Network Interface

Promiscuous Mode ☒ On ☐ Off

Filter

Example: 'ip host helios and not iceberg'

Format

## Dump File

Last created on Wed May 08 10:25:25 UTC 2019  
 FileSize : 42856 bytes  
 Format : Raw Packet Data  
 Host Name : cnmaestrostitise  
 Network Interface : GigabitEthernet 0  
 Promiscuous Mode : On  
 Filter :

[Download](#)

[Delete](#)

5. User can Navigate to Live Logs under Operations > RADIUS > Live Logs and can check the client entries which have tried to contact the ISE RADIUS service.



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
Live Sessions

Misconfigured Supplicants
0

Misconfigured Network Devices
0

Refresh
Reset Repeat Counts
Export To

	Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...
x					Identity	Endpoint ID	Endpoint Prof
	Jun 03, 2019 08:06:57.943 AM			23	anand	94:14:7A:B7:AB:B3	Unknown

Last Updated: Mon Jun 03 2019 13:37:56 GMT+0530 (India Standard Time)

- For detailed steps, Click on icon under details in Radius live logs table and will open in the new tab as shown below
- For Session trace details, please click on troubleshoot and select session trace Tests

Identity Services Engine

Home

Context Visibility

Operations

Policy

Administration

RADIUS

Threat-Centric NAC Live Logs

TACACS

Troubleshoot

Adaptive Network Control

Reports

Diagnostic Tools

Download Logs

General Tools

RADIUS Authentication Trouble...

Execute Network Device Comm...

Evaluate Configuration Validator

Posture Troubleshooting

EndPoint Debug

TCP Dump

Session Trace Tests

TrustSec Tools

Session Trace Test Cases > New

Session Trace Test Case

Test Setup

Run Test

Previous Runs

Name \*

Description

Predefined Test

Predefined test

Select type (optional)

Custom Attributes

=

Radius.Calling-Station-ID=94-14-7A-B7-AB-B3

Radius.User-Name=anand

Radius.NAS-IP-Address=10.110.200.12

Radius.NAS-Port-Type=Wireless - IEEE 802.11

Network Access.NetworkDeviceName=solution\_team

InternalUser.UserType=User

Network Access.Protocol=RADIUS

Radius.NAS-Port=214461962

Radius.Framed-MTU=1400

Summary of all attributes

Network Access.NetworkDeviceName=solution\_team

InternalUser.UserType=User

Network Access.Protocol=RADIUS

Radius.NAS-Port=214461962

Radius.Framed-MTU=1400

Radius.State=64CPMSessionID=0a6e86e53wCVALeKUZTr1f\_OYIQPwV2iKg3Qrys;39SessionID=cnmaestrositise/332254785/156;

Radius.Acct-Session-Id=58-C1-7A-36-8B-B9-B2-EA-E4-55-94-14-7A-B7-7C-4E-4A-5A

Radius.Acct-Multi-Session-Id=E6-EA-09-A8-99-C9-AC-81-E7-5C-94-14-7A-B7-7C-4E-4A-5A

WISPr.WISPr-Location-Name=BANGALORE

Network Access.AuthenticationStatus=AuthenticationPassed

DEVICE.Network Device Profile=CambiumNetworks

DEVICE.Network Device Model=CambiumNetworks

Ca

### Step 9: cnPilot Configuration

1. Navigate to WLAN > Create/Select the WLAN where “WPA2 enterprise” is enabled,
2. Select Radius server tab of the respective WLAN

Basic	Radius Server	Guest Access	Usage Limits	Scheduled Access	Access	Passpoint
<div>Authentication Server 1</div> <div>Host</div> <div>10.110.134.229</div> <div>Secret</div> <div>.....</div> <div>2</div> <div>Host</div> <div></div> <div>Secret</div> <div></div> <div>3</div> <div>Host</div> <div></div> <div>Secret</div> <div></div>						