PICAS

Pica8 Deployment Guide

PicOS[®] NAC Integration with Cisco Identity Services Engine (ISE) Node

PICAS

Contents

Cisco Identity Services Engine (ISE) Solution	1
PicOS Network Access Control – Secured Wired Access Solution	1
Deploying an ISE Node	1
Requirements	2
Use Case Overview and Topology	2
Integrating PicOS with Cisco ISE for Radius Authentication	4
Configuring the PicOS Switch	4
Configuring the ISE Node	5
Import PicOS Network Device Profile	5
Configure PicOS Network Device Profile	6
Adding a PicOS Network Device Profile	6
Verifying the Connectivity Between the PicOS Switch and ISE Node	10
Configuring an Employee Laptop with 802.1x Supplicant	11
Configure the PicOS Switch	11
Configure the 802.1X Wired Access Policy for Employee Laptop	11
Creating User Identity Group and add Users	11
Create an Authorization Profile to Dynamically Assign a VLAN	13
Create the Wired Access Policy for an Employee Lanton Running 802 1x Supplicant	13
Configuring the Windows Supplicant on the Lanton	16
Verifying the NAC Configuration	10
IP Phone Authentication	18
Configuring the MAB Wired Access policy in ISE for IP Phones	18
Contiguring the MAB Wired Access policy in ISE for IP Phones Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses	18
Configuring the MAB Wired Access policy in ISE for IP Phones Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN	18 18 19
Configuring the MAB Wired Access policy in ISE for IP Phones Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone	18 18 19 20
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication	18 18 19 20 24
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication Verifying the NAC Configuration	18 18 19 20 24 27
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication Verifying the NAC Configuration Guest Laptop Using Central Web Authentication	18 18 19 20 24 27 28
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication Verifying the NAC Configuration Guest Laptop Using Central Web Authentication Configuring the PicOS Switch	18 18 19 20 24 27 28 28
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication Verifying the NAC Configuration Guest Laptop Using Central Web Authentication Configuring the PicOS Switch Configuring the ISE Node With a Central Web Authentication Policy	18 18 19 20 24 27 28 28 28 28 29
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication Verifying the NAC Configuration Guest Laptop Using Central Web Authentication Configuring the PicOS Switch Configuring the ISE Node With a Central Web Authentication Policy Verifying the NAC Configuration	18 18 19 20 24 27 28 28 29 38
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication Verifying the NAC Configuration Guest Laptop Using Central Web Authentication Configuring the PicOS Switch Configuring the ISE Node With a Central Web Authentication Policy Verifying the NAC Configuration	18 18 19 20 24 27 28 28 29 38 29 38 42
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication Verifying the NAC Configuration Guest Laptop Using Central Web Authentication Configuring the PicOS Switch Configuring the PicOS Switch Configuring the ISE Node With a Central Web Authentication Policy Verifying the NAC Configuration	18 18 19 20 24 27 28 28 29 38 29 38 42 42
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication Verifying the NAC Configuration Guest Laptop Using Central Web Authentication Configuring the PicOS Switch Configuring the ISE Node With a Central Web Authentication Policy Verifying the NAC Configuration Troubleshooting Check Whether the ISE Server is Reachable from the PicOS Switch Check the NAC Authentication Status of all Ports	18 18 19 20 24 27 28 28 29 38 29 38 42 42 43
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication Verifying the NAC Configuration Guest Laptop Using Central Web Authentication Configuring the PicOS Switch Configuring the ISE Node With a Central Web Authentication Policy Verifying the NAC Configuration Troubleshooting Check Whether the ISE Server is Reachable from the PicOS Switch Check the NAC Authentication Status of all Ports Check VLANs to Verify Dynamic VLANs Assignment to a Port	18 18 19 20 24 27 28 28 29 38 29 38 42 42 43 44
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication Verifying the NAC Configuration Guest Laptop Using Central Web Authentication Configuring the PicOS Switch Configuring the PicOS Switch Configuring the ISE Node With a Central Web Authentication Policy Verifying the NAC Configuration Troubleshooting Check Whether the ISE Server is Reachable from the PicOS Switch Check the NAC Authentication Status of all Ports Check VLANs to Verify Dynamic VLANs Assignment to a Port	18 18 19 20 24 27 28 28 29 38 29 38 42 42 43 44 45
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication Verifying the NAC Configuration Guest Laptop Using Central Web Authentication Configuring the PicOS Switch Configuring the PicOS Switch Configuring the ISE Node With a Central Web Authentication Policy Verifying the NAC Configuration Troubleshooting Check Whether the ISE Server is Reachable from the PicOS Switch Check the NAC Authentication Status of all Ports Check VLANs to Verify Dynamic VLANs Assignment to a Port Check Dynamic ACL Rules Check Downloadable ACL Rules	18 18 19 20 24 27 28 28 29 38 42 42 42 43 44 55 46
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication Verifying the NAC Configuration Guest Laptop Using Central Web Authentication Configuring the PicOS Switch Configuring the ISE Node With a Central Web Authentication Policy Verifying the NAC Configuration Troubleshooting Check Whether the ISE Server is Reachable from the PicOS Switch Check the NAC Authentication Status of all Ports Check VLANs to Verify Dynamic VLANs Assignment to a Port Check Dynamic ACL Rules Check Trace Logs for Radius	18 18 19 20 24 27 28 28 29 38 29 38 29 38 42 42 43 44 45 46 46
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication Verifying the NAC Configuration Guest Laptop Using Central Web Authentication Configuring the PicOS Switch Configuring the ISE Node With a Central Web Authentication Policy Verifying the NAC Configuration Troubleshooting Check Whether the ISE Server is Reachable from the PicOS Switch Check the NAC Authentication Status of all Ports Check VLANs to Verify Dynamic VLANs Assignment to a Port Check Dynamic ACL Rules Check Trace Logs for Radius Reference	18 18 19 20 24 27 28 28 29 38 42 42 43 44 45 46 46 46 46
Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses Create an Authorization Profile to Dynamically Assign a Voice VLAN Create a Wired Access Policy for an IP Phone Access Point Authentication Verifying the NAC Configuration Guest Laptop Using Central Web Authentication Configuring the PicOS Switch Configuring the PicOS Switch Configuring the ISE Node With a Central Web Authentication Policy Verifying the NAC Configuration Troubleshooting Check Whether the ISE Server is Reachable from the PicOS Switch Check the NAC Authentication Status of all Ports Check VLANs to Verify Dynamic VLANs Assignment to a Port Check Dynamic ACL Rules Check Trace Logs for Radius Reference PicOS	18 18 19 20 24 27 28 28 29 38 42 42 43 44 45 46 46 46 46



Cisco Identity Services Engine (ISE) Solution

This document provides details on how to integrate and test the Cisco ISE NAC solution with PicOS[®] switches for Secured Wired Access.



ISE authenticates users and endpoints via 802.1x, Web Authentication, Mac Authentication Bypass (MAB), and other means. ISE can also query external identity sources for identity resolution and apply appropriate network policies by instructing the network devices.

PicOS Network Access Control – Secured Wired Access Solution

PicOS supports the following Secured Wired Access solutions:

· Authentication Methods: Following authentication methods are supported.

- 802.1x

- MAC Authentication Bypass (MAB or MAC-RADIUS)
- Central Web Authentication
- Multi-host support Support for multiple endpoints to be connected to the network through the same switchport
- Policy Enforcement The following network policies can be enforced:
 - Dynamic VLAN Assignment (by ID and Name)
 - Dynamic Access Control List (ACL)
 - Downloadable ACL
 - CoA (Change of Authorization)
- · Server Fail VLAN provide limited network connectivity to users in the event of AAA server failure

Deploying an ISE Node

Please refer to the following document for deploying an ISE VM using an OVA template: Cisco ISE Installation Guide Release 2.6



Requirements

This integration example uses the following hardware and software components for the policy infrastructure:

- A Dell N3048EP-ON switch running PicOS Release 4.1.2.2 (or later)
- An ISE node running release 2.6.0.156 patch 9 (or later)
- An employee laptop running Microsoft Windows 7 Enterprise
- A guest laptop running Mac OS
- A Cisco IP Phone
- An Aruba Access Point

Use Case Overview and Topology

This document provides information for the following authentication uses cases.

- 1. Employee laptop: An employee laptop with 802.1x supplicant is connected to the switch either directly or behind an IP phone and will be authenticated by an 802.1x authentication method. Both dynamic VLAN and ACL policies will be applied to the port where the employee laptop is connected. In the example configuration, the ISE node is configured to authenticate 802.1X users using its local user database. If the authenticated employee is listed in the database as belonging to the Pica8 Employee group, the ISE node returns the VLAN ID 10 to the switch in a RADIUS attribute. The switch then dynamically configures the laptop access port to be in VLAN 10. The employee laptop connected behind a Cisco IP Phone is connected to port ge-1/1/5.
- 2. IP Phone: A Cisco IP Phone is connected to port ge-1/1/5 and gets authenticated by MAB authentication method. Dynamic Voice VLAN policy will be applied to the port where the Cisco IP phone is connected. Switch configures the port to be in VLAN 800.
- Registered device: An Aruba Access Point is connected to port ge-1/1/6. We will use MAB authentication method for this endpoint. Both dynamic VLAN and Downloadable ACL policies will be applied to the port where the Access Point is connected.
- **4. Guest laptop:** A guest laptop does not have 802.1x supplicant running. We will use Central Web Authentication method for this use case. The guest laptop is connected to port ge-1/1/7. Both dynamic VLAN and ACL will be applied to the port where Guest laptop is is connected.





The following are high-level policies in ISE that we will use:

diada cisco	dentity Se	ervices Engine Home +	Context Visibility	Policy Administration	Work Centers	License W	Varning 🔺	٩
Policy	Sets Pro	ofiling Posture Client Provisionin	ng			Click here to do wireless setup and v	/isibility setu	ip Do not i
Policy	Sets					Reset Policyset	Hitcounts	R
+	Status	Policy Set Name	Description	Conditions	Policy for guests autheticating via Web,	Allowed Protocols / Server Seq	uence	Hits
Search	1				registered endpoint devices autenticating via MAB			
	\odot	Pica8-Mab-Auth		Wired_MAB	×	Default Network Access ×	- +	702
E	Ø	Pica8-Employee		Wired_802.1X	Policy for employees authenticating using Dot1x	Default Network Access ×	- +	35
	\otimes	Pica8-Registered-Device		Wired_MAB		Default Network Access ×	- +	0
	Ø	Default	Default policy set			Default Network Access ×	- +	0
								R

1. Pica8-Employee Policy: This is user based authentication and it uses an 802.1x authentication method for Employees. The following Authorization Profile is used:

a. Default: The following policies are used for employees authenticated by an 802.1x authentication method.

For more details on the Pica8-Employee policy refer to the later sections of the document.

Authorization Policy (1)									
				Result	ts				
+ si	+ Status Rule Name		Conditions	Profile	Profiles Security Groups		Hits	Actions	
Search									
			+						
	0	Default		× pic	a8-employee-acl-profile	Select from list	10	٥	

- 2. Pica8-Mab-Auth Policy: This is device based authentication and it uses Central Web Authentication for guests and uses Mac Authentication Bypass (MAB) for registered devices. The following Authorization Profiles are used:
 - a. Registered-IP-Phone rule: This rule is used for registered Cisco IP Phones
 - b. Registered-Device-Rule: This rule is used for registered AP devices
 - c. Pica8-unknown-guests: This rule is used for authenticating the guest user whose laptop will not have an 802.1x supplicant.
 - d. Pica8-known-guests: Once guest logins into the Guest Portal, this rule will be used for the registered guests.

For more details on the Pica8-Mab-Auth policy refer to the later sections of the document.



Y Authority	Authorization Policy (5)										
+					Results						
	Status	Rule Name	Cond	itions	Profiles		Hits	Actions			
Search	1										
	ø	Registered-IP-Phone	48.	IdentityGroup:Name EQUALS Endpoint Identity Groups:RegisteredDevices:Pica8-Cisco- IP-Phone	× pica8-dynamic-voice-vlan	+	Select from list	- +	25	٥	
	Ø	Registered-Device-Rule	485	IdentityGroup-Name EQUALS Endpoint Identity Groups:RegisteredDevices:AP-Group	× Pica8-downloadable-ACL × Pica8-mab-vlan-profile	+	Select from list	• +	194	٥	
	Ø	Pica8-known-guests	幽	IdentityGroup-Name EQUALS Endpoint Identity Groups:GuestEndpoints:Self_Register_Guest	× Pica8-Guest-ACL × Pica8-guest-VLAN	+	Select from list	- +	0	٥	
	Ø	Pica8-unknown-guests	484	IdentityGroup:Name NOT_EQUALS Endpoint Identity Groups:GuestEndpoints:Self_Register_Guest	× CWA_preauth	+	Select from list	- +	14	٥	
	\odot	Default			×DenyAccess	+	Select from list	× +	0	٥	

Integrating PicOS with Cisco ISE for Radius Authentication

The following sections go over PicOS and Cisco ISE configurations for Radius Authentication.

Configuring the PicOS Switch

The following sections go over the basic configuration steps in a PicOS switch needed for the Radius Authentication.

```
1. Configure VLAN interface
  set vlans vlan-id 10 vlan-name "vlan10"
  set vlans vlan-id 10 13-interface "vlan10"
  set vlans vlan-id 800
  set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 10
  set interface gigabit-ethernet te-1/1/3 family ethernet-switching port-mode "trunk"
  set interface gigabit-ethernet te-1/1/5 family ethernet-switching port-mode "trunk"
  set interface gigabit-ethernet te-1/1/6 family ethernet-switching port-mode "trunk"
  set interface gigabit-ethernet te-1/1/7 family ethernet-switching port-mode "trunk"
  set I3-interface vlan-interface vlan10 address 192.168.42.170 prefix-length 24
  set ip routing enable true
  set system inband vlan-interface vlan10
2. Provide the RADIUS server connection information
  set protocols dotlx aaa radius authentication server-ip 192.168.42.105 shared-key pica8pica8
3. Configure the access profile
  set protocols dot1x aaa radius nas-ip 192.168.42.170
4. Configure a RADIUS dynamic authorization client from which the switch accepts the Change of Authorization (CoA)
  messages. (This is optional.)
  set protocols dot1x aaa radius dynamic-author client 192.168.42.105 shared-key pica8pica8
```

5. Configure the interval for re-sending the authentication messages to the AAA server when the AAA server does not respond



during NAC authentication. Here retry interval is set to 3 seconds. set protocols dot1x aaa radius authentication server-ip 192.168.42.105 retry-interval 3

6. Configure 802.1x, MAB and multiple host mode on all access ports

The following is an example configuration for one of the access port in the PicOS switch. All ports enable the 802.1x, MAB and Web Authentication modes. Clients with 802.1x supplicant get authenticated with 802.1x while other clients get authenticated with either MAB or Central Web Authentication. Also multiple-host mode is enabled on all ports.

set protocols dotlx interface ge-1/1/5 auth-mode 802.1x set protocols dotlx interface ge-1/1/5 auth-mode mac-radius set protocols dotlx interface ge-1/1/5 auth-mode web

Configure the host mode to multiple for the interface ge-1/1/5 so that we can use multiple hosts connected to the same port (Example: laptop behind an IP phone connected to the port)

set protocols dot1x interface ge-1/1/5 host-mode "multiple"

Configuring the ISE Node

The following three configuration steps are needed to configure the ISE node for RADIUS Authentication.

- 1. Import PicOS Network Device Profile
- 2. Configure PicOS Network Device Profile
- 3. Add a PicOS switch as ISE network device

Import PicOS Network Device Profile

Cisco ISE 2.X comes with many pre-imported Network Device Profiles already on the system. The PicOS Network Device Profile is not one of these (at this time).

To import the PicOS Radius dictionary for ISE, navigate to **Policy->Policy Elements -> Dictionaries -> System -> Radius -> RADIUS Vendors**, and click Import at the top of the table as shown below.

Identity Services Engine Home	Context Vability Operations Polic	y Administration +	Work Centers	Licence Warning 📥 🔍 🔍 🔍
cy Sets Profiling Posture Client Provision	Policy Elements			
onaries + Conditions + Results				Click here to do wreeess setup and viscency setup to not show this ag
ictionaries	RADIUS Vendors			Salarant II Taul M. 🚳 🖉
[م	ten dag Marin and			Barry and an and
3 • E • ⊕•	And down Wreen Studen 9	P Expert		Stow All
 identity Mapping 	Nome	 Vervdor ID 	Description	
 IdentityGroup 	Airespace	14179	Dictionary for Vendor Airespace	
InternalCA	Alcatel-Lucent	800	Dictionary for Vendor Alcatel-Lucent	
 InternalEndpoint 	Aruba	14823	Dictionary for Vendor Aruba	
internalUser	Brocade	1588	Dictionary for Vendor Brocade	
I I I I I I I I I I I I I I I I I I I	Cisco	9	Dictionary for Vendor Cisco	
- E P	Cisco-885M	5263	Dictionary for Vendor Cisco-885H	
 ULDP 	Cisco-VPN3000	3076	Dictionary for Vendor Cisco-VPN3000	
- EI MAC	нас	25506	Dictionary for Vendor H3C	
I MON_LOG	C HP	11	Dictionary for Vendor HP	
U WSE	autoer	2535	Dictionary for Vendor Juniper	
- El ano	Monard	311	Dictionary for Vendor Microsoft	
• Li stutimedia	Advances frembed	200	Distinguist for Vendor Motorcia-Sembol	
- III NETPLOW		25053	Distinguist for Vendor Burleys	
Network Access		14122	Participany for Vendor WISDy	
Retwork Condition	C) where	14122	Distancey for venuer warr	
International Partice				
CI PROFILER				
A LUCKET				
· FADIUS Vandera				
 Lot remove to 				
 Alcatel-Lucent 				
 Antes 				
 Drocade 				
 Caso 				
 Cisco-888M 				
 Cisco-VPN3000 				
 PTT LINE 				



Click Browse and select Pica8_dictionary_ISE.xml file.

cisco identity	Services Engine	Home > C	Context Visibility	Operations	→ Policy	 Administration 	Work Centers
Policy Sets	Profiling Posture	Client Provisioning	✓ Policy Elements				
Dictionaries	Conditions	esults					
Dictionari	es	م چ	Use this for to import a Vendor file: Browse Pica8 Import Cancel	RADIUS Vend	or. Select the	e file using the browser	r and click "Import".

After importing the Pica8 RADIUS dictionary, you will see Pica8 under the Radius vendors as shown below.

dentity Services Engine Home	Context Visibility Operations Policy	Administration	Work Centers	License Warning 📤 🔍 💿 🔿
Policy Sets Profiling Posture Client Provision	ing			×
Dictionaries & Conditions & Results				Click here to do wireless setup and visibility setup Do not show this again.
Submines Positions Pressio				
Dictionaries	RADIUS Vendors			
				Selected 0 Total 15 🧐 🥪
(a + ta +) (3)	/ Edit 📥 Add 🗙 Delete 🕼 Import 🕼 Expo	rt		Show Al 🗾 🖌
 ETF Identity Mapping 	Name Name	 Vendor ID 	Description	
IdentityGroup	Airespace	14179	Dictionary for Vendor Airespace	
InternalCA	Alcatei-Lucent	800	Dictionary for Vendor Alcatel-Lucent	
InternalEndpoint	Aruba	14823	Dictionary for Vendor Aruba	
InternalUser	Brocade	1588	Dictionary for Vendor Brocade	
IOTASSET	Cisco	9	Dictionary for Vendor Cisco	
▶ 111 IP	Cisco-BBSM	5263	Dictionary for Vendor Cisco-BBSM	
ILLDP	Cisco-VPN3000	3076	Dictionary for Vendor Cisco-VPN3000	
► III MAC	Нас	25506	Dictionary for Vendor H3C	
MDM_LOG	П нр	11	Dictionary for Vendor HP	
► THE WRE	Juniper	2636	Dictionary for Vendor Juniper	
► ET WOD	Microsoft	311	Dictionary for Vendor Microsoft	
 Mutmedia STANETELOW 	Motorola-Symbol	388	Dictionary for Vendor Motorola-Symbol	
VIII Network Acress	Pica8	35098	Dictionary for Vendor Pica8	
El Network Condition	Ruckus	25053	Dictionary for Vendor Ruckus	
► EB NMAP	WISPr	14122	Dictionary for Vendor WISPr	
NMAPExtension				
Normalised Radius				
PassiveID				
Desture				
PROFILER				
* 🧰 Radius				
III IETF				
RADIUS Vendors				
Aireapace				
Alcatel-Lucent	1			

Configure PicOS Network Device Profile

To do this we will create the following Network Device Profile. PicOS – We will create a Network Device Profile called PicOS. It will cover 802.1x and MAB authentication of endpoints. PicOS switches will use this Network Device Profile.

Adding a PicOS Network Device Profile

The following are the steps needed to add the PicOS Network Device Profile:

1. Navigate to Administration->Network Resources->Network Device Profiles and add click Add. Enter Name, Description, upload Pica8 icon, select RADIUS, and select Pica8 Dictionary as shown below.



-thete Identity Services Engine Hor	me + Context Visibility + Operations + Pr	olicy + Administration + Work Centers		Ucense Warring 🔺 🤗	
+ System + Identity Management + Nel	Awark Resources > Device Portal Management pr	sGrid Services - + Feed Service - + Threat Cent	ne NAC		
Network Devlocs Network Devloc Group:	Network Device Profiles External RADIUS Service	ors RADIUS Server Sequences NAC Manage	rs External MDM + Location Services		
Nenach Device Profile List + 92005 Network Device Profile Description List Indie Vendor Unan Two Change I Vendor Supported Protocols	PICOS switches kontuu] Set To Switcu I] 40	500	Rest		
RADIUS					
TACACS+					
TristSec					

2. Expand Flow Type Conditions under the Authentication/Authorization section

- a. Select Wired MAB, and enter the conditions shown below
- b. Select Wired 802.1x and enter the conditions shown below
- c. Select Wired Web Authentication and enter the conditions shown below

diale cisco	Identity Servi	ices Engine	Home	Context	Visibility	 Operations 	Policy	→ Admi	nistration	♦ Wor	k Centers			
) ► S	ystem 🔸 Identi	ty Management		rk Resources	+ Device	Portal Management	pxGrid S	Services	Feed Sen	vice I	Threat Centric N	IAC		
► N	etwork Devices	Network Device	Groups	Network Devi	ce Profiles	External RADIUS	Servers	RADIUS	Server Seque	nces	NAC Managers	External MDM	Location Service	s
Те	mplates													
	roand All / Collans	o All												
	Authenticativ	on / Authorizati	ion											
L		Conditions												
		detected if the fel	louing oor	dition/o) oro m	at .									
	Wired WAB	detected in the for	iowing cor	iuliuon(s) are m	ы.									
	Radius:NAS	-Port-Type	0	Ethernet						÷				
			V											
	Radius:Serv	ice-Type	0	Call Check						T				
	Wireless Mi	AB detected if the	following	condition(s) are	met :									
		no detected in the	lollowing	condition(s) are	met .									
	Select an ite	em												
		in determined 20 Marco												
	Wired 802.1	ix detected if the t	roliowing c	ondition(s) are	met :									
	Radius:NAS	-Port-Type	0	Ethernet						÷				
			.											
	Radius:Serv	ice-Type	0	Framed						Ŧ				
					1.57						_			
		Wir	ed Web A	uthentication	detected if	f the following con	dition(s) are	e met :						
		Rad	lius:NAS-F	Port-Type	C	Ethernet			_	٦.		-	1	
					0									
		Rad	lius:Servio	e-Type	0	Login			-			-	÷	
					0									



3. Set Host lookup (MAB) as shown below.



4. Expand *Permissions*, select *Set VLAN* and *IETF 802.1x Attributes*. Select Set *ACL* and set it to *Radius:Filter:ID* as shown below. This will enable the dynamic filter functionality in the NAC system.

Authentication/Authorization	
▼ Permisssions	
->2 Set VLAN	
IETF 802.1X Attributes	
O Unique Attributes () ID Radius:Tunnel-Private-Group-ID () Name	
Set ACL Radius:Filter-ID	
	Jump To Top / Bottom
Change of Authorization (CoA)	

- 5. Expand CoA, select Radius for CoA and set CoA parameters as shown below. This template defines how the CoA is sent to the PicOS network device.
 - Disconnect: Select how to send a disconnect request to these devices.
 - Select RFC 5176 under Disconnect and set parameters as shown below.
 - Port Bounce: Select how to send a Port Bounce request to these devices.
 Select Port Bounce: Check box to terminate the session and restart the port, and enter parameters as shown below. Set the Pica8:Pica8-AVPair value is set to command=pica8-bounce-host-port
 - Port Shutdown: Select how to send a Port Shutdown request to these devices.
 - Select *Port Shutdown*: Check box to terminate the session and shutdown the port and enter parameters as shown below. Set the *Pica8:Pica8-AVPair* value to *command=pica8-disable-host-port*



dentity Ser	vices Engine	Home	Context	Visibility	 Operations 	▶ Policy	▼ Adm	inistration	→ Wo	ork Centers	
Iden → System → Iden	tity Management	Network	Resources	Device F	Portal Management	pxGrid	Services	Feed Se	rvice	Threat Centric I	NAC
 Network Devices 	Network Device	Groups	Network Devi	ce Profiles	External RADIUS	Servers	RADIUS	Server Sequ	ences	NAC Managers	E
✓ Change of I	Authorization (C	CoA)									_
CoA by RADI	US		•								
	* Default CoA Port	3799		D							
* Defa	ult DTLS CoA Port	2083		D							
	* Timeout Interval	5	s	econds (j)							
	* Retry Count	3	(Ð							
Send Mess	age-Authenticator										
Disconnect											
RFC 5176											
Radius:Acct-	Terminate-Cause	A	dmin Reset						÷		
Port Bounce	9										
Pica8:Pica8-	AVPair	© = ∞ ⊙	ommand=pica	8-bounce-ho	st-por				÷		
Radius:Acct	Terminate-Cause	⊘ = A	dmin Reset						÷		
Port Shutdo	wn										
Pica8:Pica8-	AVPair	© [−] 00	ommand=pica	8-bounce-ho	st-por	7			÷		
Radius:Acct	Terminate-Cause	A	dmin Reset						÷		

6. Expand *Redirect*, enter the values as shown below.

dentity Services En	gine _{Home}	Context Visibility	Operations Policy	✓ Administration → V	Vork Centers
System Identity Management	gement - Netwo	rk Resources > Device	ce Portal Management pxGri	d Services Feed Service	Threat Centric
Network Devices Network	rk Device Groups	Network Device Profile	s External RADIUS Servers	RADIUS Server Sequences	NAC Managers
CoA Push					
RFC 5176					
Select an item	◎ =		-		
Redirect					
Type Dynamic URL					
Pica8:Pica8-Redirect-U	irl 📀	= \${URL}			
		Dynamic URL P	arameter		
		Session ID			
		Olient MAC A	ddress		
		O None			
Redirect URL Parame	ter Names				
Client IP Address					
Client MAC Address	mac				
Originating URL					
Session ID					
SSID					



7. Lastly, click Submit to save the PicOS Network Device Profile.

Adding a PicOS switch as ISE Network Device

To add a PicOS switch to the Network Device database, navigate to *Administration ->Network Resources->Network Devices* and add a new device as shown below. Make sure to enter values for the following fields: *Name, IP address, Model Name* and *Software version*.

Next set PicOS as the "Device Profile".

Enter the shared secret value *pica8pica8* as configured in the PicOS switch. Click *Submit* to save the Network Device configuration.

In 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 Location Services
Network Devices
Name Branch-A-Access-Switc
Default Device Description
Device Security Settings
1P Mulless * IP: 192.100.42.170 / 22
* Device Profile 💥 PICOS 👻 🕀
Model Name N3248P-ON *
Software Version 4.1.2.2
* Network Device Group
Location All Locations 📀 Set To Default
IPSEC No Set To Default
Device Type All Device Types O Set To Default
RADIUS Authentication Settings
RADIUS UDP Settings
Protocol RADIUS
* Shared Secret Show
Use Second Shared Secret 🔲 🕡
Show
CoA Port 3799 Set To Default
RADIUS DTLS Settings ()
DTLS Required 🔲 👔
Shared Secret radius/dtls (i)
CoA Port 2083 Set. To Default

Verifying the Connectivity Between the PicOS Switch and ISE Node

Verify PicOS switch reachability to the ISE node using the following CLI command:

admin@P8-Access	-BR-1-SW-	2> show a	lot1x	server					
Server-IP	-IP Status Priority Retry-Interval		Retry-Num	Det	ect-Interval	Consecutive-Detect-Num			



Configuring an Employee Laptop with 802.1x Supplicant

In this example configuration, the Cisco ISE node is configured to authenticate 802.1x users using its local user database. If the authenticated employee is listed in the database as belonging to the *Pica8 Employee* group, ISE returns the VLAN ID 10 to the switch in a RADIUS attribute. ISE also returns the *mac_auth_policy_2* dynamic ACL for employees. The switch then dynamically configures the laptop to be in VLAN 10 with *mac_auth_policy_2* ACL. The Cisco IP Phone is connected to port *ge-1/1/5* with the employee laptop connected behind the Cisco IP Phone.

This use case involves configuring the PicOS switch, configuring the ISE node, configuring the windows supplicant on the laptop, and then verifying the NAC configuration.

Configure the PicOS Switch

Configure the Dynamic ACL to be used when an employee laptop is connected to the switch. set protocols dot1x filter mac_auth_policy_2 sequence 999 then action forward

Configure the 802.1x Wired Access Policy for Employee Laptop

Configuring the 802.1x Wired Access policy in ISE for Employee laptop involves the following four steps:

- 1. Create User Identity groups and integrate with AD or add local users
- 2. Create an Authorization Profile to dynamically assign VLAN 10 for employee laptops running 802.1x supplicant
- 3. Create an Authorization Profile to dynamically assign an ACL called mac_auth_policy_2 to the employee laptops that will provide full corporate network access
- 4. Create a Wired Access policy for Employee Laptop running 802.1x supplicant (called Pica8-Employee) that will use the above two authorization profiles

Creating User Identity Group and add Users

Cisco ISE allows for Active Directory integration. Here we will use local groups and users defined in ISE for this integration test. To add a group, navigate to *Administration -> Identity Management->Groups->User Identity Groups* and click + as shown below.

ciaco Identity Services Engine Home	Context Visibility	Istration	Libense Warning 🔺 🤍 🎯 😁 🐡
System Videntity Management Network Re	sources > Device Portal Management pxGrid Services	Feed Service Threat Centric NAC	
Identities Groups External Identity Sources	Identity Source Sequences		
Identify Crouns			
Adentity droups	User Identity Groups		Protocol & L. Tatal & 🦓 🏤
	/ Edit dia Add X Delete v @bilmport @b Export v		Show All
Endpoint Identity Groups	Name	Description	
Liser Identity Groups	ALL ACCOUNTS (default)	Default ALL ACCOUNTS (default) User Group	
	Employee	Default Employee User Group	
	GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group	
	GuestType_Contractor (default)	Identity group mirroring the guest type	
	GuesfType_Daily (default)	Identity group mirroring the guest type	
	GuestType_SocialLogin (default)	Identity group mirroring the guest type	
	GuestType_Weekly (default)	Identity group mirroring the guest type	
	OWN_ACCOUNTS (default)	Default OWIN_ACCOUNTS (default) User Group	
	Pica8-Employees	Employees of PicaB	

Enter Name and Description of the Group as shown below and click Submit.



"livel" Identity Services Engine Home	Context Visibility	License Warning 🔺 🔍 💿 🗢 🗢
System Identity Management Network Re Identities Groups External Identity Sources	sources	Click here to do wireless setup and visibility setup Do not show this again.
Identity Groups	User Identity Groups > Pice8-emp	
	Identity Group	
CE COUP CE COUP CE COUP CE COUP CE COUP CE COUP	Description Pica8 Employees	<i>l</i> h

To add a user, navigate to Administration -> Identity Management->Identities and click + as shown below.

dentity Services Engine	Home	Policy Administration	 Work Centers 		License Warning	🔺 < (9 0 0
 System Identity Management 	Network Resources Device Portal Manager	ment pxGrid Services + Feed Services	vice				
- Identities Groups External Identit	ty Sources Identity Source Sequences + Set	tings					
0							
Users	Network Access Users					Selected 0	Total 1 🚳 🚳
Latest Manual Network Scan Results	/ Edit - Badd - Michannes Status - Philm	nort (Th Event - Pallite - Pallite	nlicate		Show All	00000000	v 192
	V cor - vido Bardiange Status +	por grephr + Aperte + allo	produc		OIOW AI		U
	Status Name	 Description First 	t Name Last Name	Email Address	User Identity Groups Ad	lmin	
	🗌 🛃 Enabled 🙎 jdoe	Joh	n Doe	jdoe@pica8.com	Pica8-Employees		

Enter *Name, Email, Login Password* and select *Pica8-Employees* for *User Groups* as shown below and click *Submit*. In this example we are adding *Network Access User* account for John Doe.

dialia cisco	Identity Service	es Engine	Home	Context Vis	sibility > Op	erations	Policy	→ Adminis	stration	Work Cente	ers	
 Syst 	em 🔽 Identity	Management	Network F	Resources	Device Portal N	lanagement	pxGrid S	ervices >	Feed Service	► Threat	t Centric NAC	
✓ Ident	tities Groups	External Identi	ty Sources	Identity Sou	rce Sequences	 Settings 						
Users Latest M	lanual Network S	Can Results	Network Network Network Network State Err Pat	twork Access twork Access twork Access twork Access two	List > jdoe s User bled + a8.com Internal User Password	S	•	Re-Enter Par	ssword		Congrate Password	
			• Lo	ogin Password	•••••			•••••			Generate Password	۲.
			Ena	able Password							Generate Password	(i)
			Ψ U	ser Informa	tion		_					
			Firs	st Name John	n]]					
			- A	ccount Optio	ons							
			Chi	ange password	Description []						li
			↓ A	ccount Disal	ble Policy	ds 2021-12-	-21		(yyyy-mr	m-dd)		
			U U	ca8-employee		◙-+						



Create an Authorization Profile to Dynamically Assign a VLAN

To create the Authorization Profile, navigate to *Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles* and click + as shown below.

cisco Identity Services Engine	Home	Operations Policy Administration	Work Centers	License Warning 🔺 🔍 🛞 💿 🌞
Policy Sets Profiling Posture Clien	t Provisioning Policy Elements			
Dictionaries + Conditions - Results				
G				
 Authentication Authorization 	Standard Authorization Pr For Policy Export go to Administrat	ofiles ion > System > Backup & Restore > Policy Expo	t Page	Selected 0 Total 11 😵 🙀 🖕
Authorization Profiles	/ Edit - 👫 🔂 🖓 Duplicate 🔰	C Delete		Show All
Downloadable ACLs	Name Name	Profile	 Description 	
Downbadable ACEs	Generic Guest Access	r PICOS 🕀		
Profiling	Pica8-Vlan10	PICOS 🕀	Assigns Vlan 10 to Pica8 EMployees	
Posture	pica8-vlan-acl-profile	F PICOS 🙂		
	Blackhole_Wireless_Access	🔐 Cisco 🕀	Default profile used to blacklist wireless	devices. Ensure that you configure a BLACKHOLE ACL on the V
Client Provisioning	Cisco_IP_Phones	🟥 Cisco 🕀	Default profile used for Cisco Phones.	
	Cisco_Temporal_Onboard	🚓 Cisco 🕀	Onboard the device with Cisco temporal	agent
	Cisco_WebAuth	🏥 Cisco 🕀	Default Profile used to redirect users to t	he CWA portal.
	NSP_Onboard	🚢 Cisco 🕀	Onboard the device with Native Supplica	ant Provisioning
	Non_Cisco_IP_Phones	🟥 Cisco 🕀	Default Profile used for Non Cisco Phone	05.
	DenyAccess		Default Profile with access type as Acces	ss-Reject
	PermitAccess		Default Profile with access type as Acces	sa-Accept

Enter *Name, Description*, set *Access Type to ACCESS_ACCEPT*, and set *Network Device Profile* to *PicOS*. Check the box for *VLAN* and enter an attribute value that identifies a VLAN. In this example VLAN ID 10 is used. Click *Submit*.

dinih cisco	Identit	y Service	s Eng	jine	Home	→ Co	ntext Visibility	/ → C	perations	- Policy	Administration	1 I	Work Centers		
Polic	cy Sets	Profiling	Pos	ture	Client Prov	risioning	▼ Policy Ele	ements	1						
Dicti	onaries	▶ Condit	tions	- Resu	ults										
				•	•										
> Aut	henticati	on			Autho	orization F	Profiles > pica	8-emplo	yee-vlan-p	rofile					
- 4.14	horizotio	-			Aut	norizati	on Pronie			n n filo					
• Aut	norizatio	n				_	Name	picas-em	pioyee-vian	-pronie					2
Au	thorizatio	n Profiles					Description				1			 ///	8
Do	wnloadab	le ACLs				• Ac	cess Type	ACCESS_/	ACCEPT	7					
Pro	filing				Ne	work Dev	ice Profile	C PICO	S 🕶 🕀	1					
Pos	ture						_			-					
> Clie	nt Provis	lioning				Commo	Tasks								
							- Tubito								
						Securit	y Group								
						VLAN		Tag ID	1	Edit	Tag ID/Name 10				
									•						
					*	Advance	d Attribute	s Settir	as						
					10	Colort or							4		
					= [select an	item		<u> </u>			<u> </u>	T		
					¥ 1	Attribut	es Details	CCEPT							
					Tu	nnel-Priva	te-Group-ID	= 1:10							
					Tu	nnel-Medi	um-Type = 1:	:6							
			_												-

Create an Authorization Profile to Dynamically assign an ACL

To create an Authorization Profile, navigate to *Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles* and click +.



Enter *Name, Description*, set *Access Type to ACCESS_ACCEPT*, set *Network Device Profile* to *PicOS*. Check the box for *ACL* and enter value for ACL. In this example mac_auth_policy_2 is used. Click *Submit*.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Clie	Int Provisioning Policy Elements
Dictionaries Conditions Results	
Authentication Authentization Authorization Authorization Profiles Downloadable ACLs Profiling Posture	Authorization Profiles > pica8-employee-act-profile Authorization Profile *Name pica8-employee-act-profile Description ////////////////////////////////////
Client Provisioning	Common Tasks ACL (Filter-ID) mac_auth_policy_2 Security Group
	Advanced Attributes Settings
	Select an item 💿 = 💿 — 🕂

Create the Wired Access Policy for an Employee Laptop Running 802.1x Supplicant

Cisco ISE is a policy-based, network-access-control solution that offers network access policy sets, thus allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type and similar parameters.

Let us create a *Policy Set* called *Pica8-Employee* to authenticate *Wired 802.1X* users and place the users on VLAN 10 and apply *mac_auth_policy_2* ACL. Navigate to *Policy -> Policy Sets* and click *+* as shown below.

cisco	ientity Se	rvices Engine Home 🕠	Context Visibility • Operation	ations • Poli	> Administratio	Work Centers			<u>1</u>	cense Warning	A 0	e	0	- 4
Policy S	Sets Pro	filing Posture Client Provisionin	g > Policy Elements											
Policy	Sets								Re	setAll Hitcou	ints	Reset	s	lave
. e	Status	Policy Set Name	Description	Condi	tions				Allowed Protocols / Ser	ver Sequence	Hits	Acti	ons	Viev
Search														
	Ø	Pica8 Employee			Wired_802.1X				Default Network Access	x * +	5	<	ŀ	>
	0	General Guest Access			Wired_MAB				Default Network Access	×* +	246	<	ł	>
	ø	Default	Default policy set						Default Network Access	x - +	1	\$	F	>

Enter *Policy Set* name as *Pica8_Employees* and click + *sign* under *Conditions, drag Wired_MAB* to the shaded box and click *Use*.



-the she Gasta	Identity Sr	envices Engine	Home + Context Visibility + Operations	Policy Admin	istration + 1	Nork Centers					Uceree	Warning 🔺	- Q.	0 0	ſ
Policy			Conditions Studio							0	×				
Polic	y Sets		Library		Editor							Hitcount		int Sav	
۲	Status	Policy Set Name	Search by Name			Click to add an attrib	uto			•		quence	Hits A	Actions Vie	ł
Bear				10 t 9	F	Equals •	Attribute	value							
1			Catalyst_Switch_Local_Web_Authen	vicat @										°)	
			Switch_Local_Web_Authentication	Ø		-	+	New AND						0 3	
			Switch_Web_Authentication	Ø	Dr	ag it to the shade	d box	OR	-						l
			Wred_802.1X	0										× ,	
			Wired_MAB	Ø										set Sav	l
			Wireless_802.1X	Ø											
			Wreless_Access	Ø											
			Wreless_MAB	Ø											
			WLC_Web_Authentication	Ø											
										\mathbf{X}					
									Clos	D 🐫					

Set Allowed Protocols to Default Network Access, click Save and click > sign as shown below.

cisco	Ident	tity Service	s Engine Home +	Context Visibility Operations	- Polic	y Administration	Work Centers				Lice	inse Waming	۹ م	0	•	ø
Pol	icy Sets	Profiling	Posture Client Provisionin	ng												
Pol	icy Se	ets									Rese	tAll Hitcou	nts	Reset	Sa	ve
	s	tatus Pol	icy Set Name	Description	Condi	tions				Allowed Protocol	s / Serve	r Sequence	Hits	Action	s Vi	iew
Se	arch															
		Pic	a8 Employee			Wired_802.1X				Default Network A	ccess	ж× +	5	٥	*	>
		⊘ Ge	neral Guest Access			Wired_MAB				Default Network A	00668	* * +	246	٥	1	>
		O Def	lault	Default policy set						Default Network A	00888	* * +	1	٥	;	>

Set Authentication Policy Options as shown below. Set Authorization Policy to Pica8-employee-acl-profile and Pica8-employee-VLAN-profile as shown below. Click Save.



cisco Id	entity Se	rvices Engine Home +	Context Visibility	Policy > Administration > Work Centers		License Warning 🔺 🤇	λ Θ	• •
Policy S	ets Prof	filing Posture Client Provisionin	g Policy Elements					
Policy	Sets →	Pica8-Employee				Reset Policyset Hitcounts	Reset	Save
	Status	Policy Set Name	Description	Conditions		Allowed Protocols / Serve	r Sequen	e Hits
Search								
	ø	Pica8-Employee		Wred_802.1X		Default Network Access	ж т	• •
❤ Auth	entication	n Policy (1)						
+	Status	Rule Name	Conditions			Use	Hits	Actions
Searc	h			L.				
				÷	_	-	_	
						All_User_ID_Stores × v		
						✓ Options		
						If Auth fail		
	0	Defect				REJECT × *		*
	۲	Delaut				If User not found	Ľ	*
						REJECT × *		
						If Process fail		
						DROP × *		
> Auth	orization	Policy - Local Exceptions						
> Auth	orization	Policy - Global Exceptions						
❤ Auth	orization	Policy (1)						
					Results			
+	Status	Rule Name	Conditions		Profiles	Security Groups	Hits	Actions
Searc	h							
				+				
	~				× pica8-employee-acl-profile			
	\odot	Default			+ pica8-employee-vlan-profile	Select from list	0	\$

Configuring the Windows Supplicant on the Laptop

On the Windows laptop enable 802.1X PEAP authentication for the Local Area Connection.

Under *Control Panel > Network and Sharing Center > Change Adaptor Settings*, right-click *Local Area Connection* and then click *Properties*. On the *Authentication* tab of the Local Area Connection Properties window, configure the properties as shown.

Organize Disable this network device	Diagnose this connection Rename this connection	View stat
Local Area Connection Network 3 Intel(R) PRO/1000 MT Network C	Local Area Connection Properties Networking Adhenicasion Sharing Select this option to provide authenticated network access for the Ethernet adapter. Probe IEEE 802 1X authentication Choose a network authentication method: Microsoft: Protected EAP (PEAP) Setting Premember my credentials for this connection each time Im logged on Palback to unauthorized network access Additional Settings. OK Call	



Click *Settings* to display the Protected EAP Properties window. In the Protected EAP Properties window, click *Configure* to configure the Secured password (EAP-MSCHAP v2). Set the *Automatically use my Windows logon name and password* check box. Credentials for the laptop are the same as the credentials stored on the ISE server.

If your ISE node is configured to use Windows Active Directory to authenticate users, you would leave this option selected.

Click *OK*. It will trigger a login screen. Enter the user ID jdoe and password of the local user that you added to local user database on the ISE server.

Verifying the NAC Configuration

After connecting the Employee Windows laptop to the Cisco IP Phone, authenticate the user *jdoe* with login credentials that we configured earlier in the ISE node database. After Authentication, make sure you are able to reach www.example.com from a browser application.

On the PicOS switch run the following CLIs to verify the 802.1x NAC configuration.

To check the 802.1x authentication run the following CLI:

admin@P8-Access-BR-1-SW-2> show dot1x interface gigabit-ethernet ge-1/1/5
Interface ge-1/1/5:

Client MAC
Status
Success Auth Method
Last Success Time
Traffic Class
Dynamic VLAN ID
Dynamic Filter Name
Status Success Auth Method Last Success Time Traffic Class Dynamic VLAN ID Dynamic Filter Name

To view real-time authentication summary in ISE, navigate to *Operations->RADIUS->Live Logs* and click on the icon under the *Details* column as shown below.

diale Identi	ity Services Engine	Home + Cont	text Visibility	- Operations	Policy	+ Administration	Work Centers						License W	aming 🔺 🔍
▼RADIUS	Threat-Centric NAC Live	e Logs	 Troublesho 	ot + Adaptive	Network Control	Reports						Click here to do	wireless setup and vi	sibility setup Do n
Live Logs	Live Sessions													
		Misconfigured Supp	licants ()	Mis	sconfigured Net	work Devices 0		RADIUS Drops €) c	lient Stopped Resp	onding	Re	peat Counter	
		0			0			0		0			2	
										R	efresh Novor	~ Show	Latest 20 records	~ Within L
C Refresh	Reset Repeat Cou	unts 💄 Export To	•											
Time		Status	Details	Repeat	Identity	End	point ID	Endpoint P	Authentication Policy	Authorizati	Authorization I	Profiles		IP Address
×			Y.		Identity	End	Ipoint ID	Endpoint Profi	Authentication Policy	Authorization	Authorization P	rofiles		IP Address
Oct 1	3, 2021 01:18:09.765 PM	0	ò	0	jdoe	80:E	8:2C:B9:28:DB	HP-Device	Pica8-Employee >> Default	Pica8-Emplo	pica8-employee-	acl-profile,pica8-empl	loyee-vian-profile	
Oct 1	3, 2021 01:18:09.707 PM		ò		jdoe	80:E	8:2C:89:28:DB	HP-Device	Pica8-Employee >> Default	Pica8-Emplo	pica8-employee-	-acl-profile,pica8-empl	loyee-vlan-profile	
Oct 1	3, 2021 01:18:08.833 PM	0	0			80:E	8:2C:B9:28:DB							
Oct 1	3, 2021 01:14:50.166 PM	0	0	2	18:5A:58:1D:9	C:21 18:5	A:58:1D:9C:21	Dell-Device	Pica8-Web-Auth >> Pica8	Pica8-Web	CWA_preauth			
Oct 1	3, 2021 01:14:47.201 PM	~	0		18:5A:58:1D:9	C:21 18:5	A:58:1D:9C:21	Dell-Device	Pica8-Web-Auth >> Pica8	Pica8-Web	CWA_preauth			
Oct 1	3, 2021 01:14:41.271 PM	2	0		18:5A:58:1D:9	C:21 18:5	A:58:1D:9C:21	Dell-Device	Pica8-Web-Auth >> Pica8	Pica8-Web	CWA_preauth			
Oct 1	3, 2021 01:14:41.155 PM	~	0		80:E8:2C:B9:2	8:DB 80:E	8:2C:B9:28:DB	HP-Device	Pica8-Web-Auth >> Pica8	Pica8-Web	CWA_preauth			
Oct 1	3, 2021 01:14:37.964 PM	0	o			80:E	8:2C:B9:28:DB							
Oct 1	3, 2021 01:14:37.132 PM	۰	0			80:E	8:2C:B9:28:DB							



Clicking the icon under the *Details* column opens the *Authentication Detail Report* in a new browser window. This report offers information about authentication status and related attributes, and authentication flow.

Overview	
Event	5200 Authentication succeeded
Username	jdoe
Endpoint Id	80:E8:2C:B9:28:DB 🕀
Endpoint Profile	HP-Device
Authentication Policy	Pica8-Employee >> Default
Authorization Policy	Pica8-Employee >> Default
Authorization Result	pica8-employee-acl-profile,pica8-employee-vlan-profile

IP Phone Authentication

A Cisco ISE node is configured to authenticate IP phone Endpoint Groups with MAB authentication. Here the Cisco IP Phone is connected to port *ge-1/1/5*, and voice VLAN 800 is configured on the PicOS switch.

Configuring the MAB Wired Access policy in ISE for IP Phones

Configuring the MAB Wired Access Policy in ISE for IP Phones involves following three steps:

- 1. Create an IP-Phone Endpoint Identity Group and add IP Phone Mac addresses.
- 2. Create an Authorization Profile to dynamically assign voice VLAN 800 for IP Phones.
- 3. Create a Wired Access policy for the IP Phone that will use the above authorization profile.

Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses

To create *IP_phone* Endpoint Identity Group , navigate to *Administration -> Identity Management -> Groups -> Endpoint Identity Groups-> Registered Devices* and click + as shown below.



dentity Services Engine Home	Context Visibility Operations Policy	Administration Vork Centers
System Identity Management Network	Resources + Device Portal Management pxGrid Serv	rices + Feed Service + Threat Centric NAC
Identities Groups External Identity Sources	Identity Source Sequences	
Identity Groups	Endpoint Identity Groups	
Endoniat Identity Groups	Name	Description
User Identity Groups	Name	Description
		Identity Group for Profile: Analoid
		Identity Group for Profile: Apple-IDevice
		Identity Group for Profile: Axis-Device
		Dentity Group for Profile: blackberry
		Blacklist Identity Group
	Cisco-IP-Phone	Identity Group for Profile: Clisco-IP-Phone
		Identity Group for Profile: Cisco-Meraki-Device
		DownloadsbieACLMAB
	Epson-Device	Identity Group for Profile: Epson-Device
	Guestendpoints	Guest Endpoints Identity Group
	L IP-Phone	Cisco IP Phone
	Juniper-Device	Identity Group for Profile: Juniper-Device
		Profiled Identity Group
	RegisteredDevices	Asset Registered Endpoints Identity Group
	Sony-Device	Identity Group for Profile: Sony-Device
	Synology-Device	Identity Group for Profile: Synology-Device
	Trendnet-Device	Identity Group for Profile: Trendnet-Device
	Unknown	Unknown Identity Group
	Vizio-Device	Identity Group for Profile: Vizio-Device
	U Workstation	Identity Group for Profile: Workstation

Enter *Name, Description* and click *Submit*. Select Pica8-Cisco-IP-Phone Groups and click + and select the MAC address of the IP phone to add IP Phone to this Endpoint Identity Group as shown below.

dentity Services Engine	Home >	Context Visibility	 Operations 	Policy Admi	nistration V	/ork Centers	
System Identity Management	Network Res	sources + Device	Portal Management	pxGrid Services	 Feed Service 	Threat Centric NAC	
Identities Groups External Identit	y Sources	Identity Source Seq	uences + Settings				
Identity Groups	م چر	Endpoint Identity Endpoint Iden • Name Description Parent Group Save Identity Group	Group List > Pica8-d ntity Group Pica8-Cisco-1P-Phor RegisteredDevices Endpoints Remove +	Claco-IP-Phone			<u> </u>
Unknown		MAC Addres	\$5	Static Group Ass	ignment	EndPoint Profile	
User Identity Groups		00:C1:B1:E	5:0A:F6	true		Cisco-Device	

Create an Authorization Profile to Dynamically Assign a Voice VLAN

To create an Authorization Profile, navigate to *Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles* and click + as shown below.



cisce Identity Services Engine	Home + Context Visibility + Operation	Policy Administration	ark Cantara Lisense Werning 🔺 🔍 💿 🔇	0
Policy Sets Profiling Posture C	Hent Provisioning Plaiky Elementa			
Dictionation + Conditions + Resul	ta			
0				
Authentication	Standard Authorization Profiles For Polky Open go to Administration > Sys	em > Backup & Rectore > Policy Export P	Selected O Traw 11 🌚	÷.
	/ B.R. + A Querre X Deere		Show All	18
Automation Promite	Nama	Profile	. Descriptor	
Downloadable AcLs	Generic Guest Access	F PICOS (E)		
Profiling	Pice8-Vian10	PICOS 🖯	Analgen Vien 10 to Picali EMployees	
Posture	pical-vian-aci-profile	F PICOS (8)		
	Blackhole_Wireless_Access	dag Cisco 🕀	Default profile used to blackist wireless devices. Ensure that you configure a BLACKHOLE ACL-	on the 1
Client Provisioning	Gaco_P_Phones	🚓 Gace 🕀	Defeat, profile used for Gazo Phones.	
	Caco_Temporal_Onispard	🚓 Carco 🕀	Drizoard the device with Cado temporal agent	
	Cisco_WebAuth	dia Cisco 🕀	Default Profile used to redirect users to the CWA portal.	
	NSP_Onboard	dia Giaco 🕀	Onsoard the device with Native Supplicant Provisioning	
	Non Class IP Phones	dia Class (i)	Default Profile used for Non Class Phones	
	DanyAccess		Default Profile with access type as Access-Reject	
	PermitAccess		Default Profile with access type as Access-Accept	

Enter *Name, Description*, and set *Access Type to ACCESS_ACCEPT*, then set *Network Device Profile to PicOS*. Check the box for *VLAN* and enter an attribute value that identifies a VLAN. In this example VLAN ID 800 is used for Voice VLAN. Expand *Advanced Attribute Settings* select *Pica8:Pica8-AVPair* and set the value as *pica8-traffic-class=voice*. Click *Submit*.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture C	ient Provisioning Policy Elements
Dictionaries Conditions Result	
0	
Authentication	Authorization Profiles > pica8-dynamic-voice-vian
	Authorization Profile
- Authorization	* Name pica8-dynamic-voice-vlan
Authorization Profiles	Description
Downloadable ACLs	* Access Type ACCESS_ACCEPT *
Profiling	Network Device Profile 20 PICOS + E
⊁ Posture	
Client Provisioning	
	▼ Common Tasks
	VLAN Tag ID 1 Edit Tag ID Name 800
	Web Redirection (CWA, MDM, NSP, CPP)
	Advanced Attributes Settings
	Pica8:Pica8-AVPair 💿 = pica8-traffic-class=voice 💿 — 🕂
	a Mada da Batala
	Access Type = ACCESS ACCEPT
	Turnel-Private-Group-ID = 1:800
	Turnel-Medium-Type = 1:6
	Micad-MMMair = picad-d'arrit-ciads=volice
	Save Reset

Create a Wired Access Policy for an IP Phone

Let us create a *Policy Set* called *Pica8-Mab-Auth* to authenticate various *Endpoint Identity Groups* using *MAB* authentication. We will place the IP Phones on voice VLAN 800. Navigate to *Policy -> Policy Sets* and click + as shown below.

-data-	identity Se	arvices Engine Home + I	Context Visibility + Operations	• Pole	Y Administration	+ Work Centers							Line	un Alecci	11 A	<i>a</i> ,	• •	
Peky	Sels Pr	offing Posture Client Provisionin	g Policy Elements															
Policy	Sets												Reset	All Hito	ounts	Re	ant (Sav
۲	Status	Policy Set Name	Description	Condi	ions						Allowed P	otocois /	Server	Bequen	ce i	in i	Actiona	Vie
Search	h																	
	0	Pica8 Employee			Wired_802.1X						Default N	hwork Acc		**	+	5	۰	;
	0	General Guest Access			Wired_MA8						Default N	hwork App		**	+	146	٥	,
	0	Defeat	Default policy set								Default N	hwark Aza		••	•	1	٥	,



Enter the *Policy Set* name as *General Access* and click + sign under *Conditions*, drag *Wired_MAB* to the shaded box and click *Use*.

	Conditions Studio						© ×	Do not show this again.
olicy Sets	Library	Editor						Result Ser
+ Status Policy	Search by Name		Click to add a	n attribute				Hits Actions Vi
Beach	♥ □ ○ ▲ ● ₽ ₽ ₽ ∞ 2 ≣ © 1 ● Ł	ę ۲	Equals	Attribute vi	ເບັດ			
 O New 1 O New 1 	Catalyst_Switch_Local_Web_Authenticati @							•
© Press	Switch_Local_Web_Authentication		*	+ (N	W AND OR			
() D()	Switch_Web_Authentication							
	Wred_802.1X 0							
	Wired_MAB 0							Resot
	Wireless_802.1X							
	Wreless_Access							
	Wreless_MAB Ø							
	WLC_Web_Authentication							
						×		
							<u>_</u>	

Set Allowed Protocols to Default Network Access, click Save and click > sign as shown below.

diselis cisco	Identity S	ervices Engine	Home	Context Visibility	Operations	* Polic	Administration	1	• Work Ce	k Centers																Lice	ise Warr	ing 🔺	٥,	θ	0	ø	l
Polic	y Sets Pr	rofiling Posture	Client Provision	ing	ents																			Click here t	do wirele	is setup	and visit	iity setu	p Do not	show th	s agai	n. ×	
Polic	y Sets																								Rese	Policy	set Hit	ounts	R	eset	S	ave	
+	Status	Policy Set Name	•	Description		Conditi	ions																	Allowed P	rotocols	Server	Seque	ce	Hits	Action	s \	View	
Sea	rch																																
	ø	Pica8-Mab-Auth]				Wired_MAB																	Default N	twork Acc	555	х т	+	298	٥	À	>	
	0	Pica8-Employee				•	Wired_802.1X																	Default N	twork Acc	255	× •	+	0	¢		>	
	\oslash	Pica8-Registered-I	Device				Wired_MAB																	Default N	twork Acc	155	× •	+	0	¢		>	
	ø	Default		Default policy set																				Default N	twork Acc	155	× *	+	0	٥		>	
																													R	eset	S	ave	

Set *Authentication Policy Options* as shown below. Create a new rule under *Authorization Policy* called *Registered-IP-Phone*. Click + sign under *Conditions*. In the *Attribute* field, search for the string *name* and then select the *IdentityGroup Name* attribute as shown below.

brar	y		Editor																																			
Sea	rch by Name			Clic	k lo add	an altrib	ute											1																				
9		0 E 🕈	Ŀ	Select	Select attribute for condition													×																				
	BYOO_is_Registered	Ø		•	53	0 4			2 0	F		2		1	0	Ŀ	÷																					
8	Catalyst_Switch_Local_Web_Authentical	Ø			Did	ionary				Attribu	te			ID		Info																						
-	Compliance_Urknown_Devices	Ø			A	Dictionari	es v		٠	nama Cerne	U.U.A.S	APRAGE	WEDVIM.	10		ω																						
8	Compliant_Devices	Ø			OP	CE				Model I	Name					ø																						
8	EAP-MSCHAPv2	Ø		Ŧ	Gue	at .				Fistra	na					Ø																						
-	EAP-TLS	Ø		1	Gue	91 92				Lasiner	ne me					0																						
8	Guest Flow	Ø		5	не					HP-Cgr	100-VL	AN-Name		65		Ø		i																				
-		-			ider	EtyGroup				Name						Ø		ł																				
	MAC_in_SAN	Q																						T	inte	nalUser				Finina	ne					۵		
	Network_Access_Authentication_Passed	Ø		Ŧ	Inte	nalUser				Lestner	ne					0																						
	Non Cisco Profiled Phones	Ø														~																						

Select Endpoint Identity Groups:RegisteredDevices:Pica8-Cisco-IP--Phone as shown below and click Save.



Conc	litions Studio						G
ibraŋ	1		Editor				
Sear	ch by Name			IdentityGroup-Name			6
9 🖘		0 t 🕫	-48-	Equais ~	× Endpoint Identity Groups:RegisteredDevices:Pica8	-Cisco-IP-P	5
	BYOD_is_Registered	Ø		Set to 'Is not'		Duplicate Sa	ave
	Catalyst_Switch_Local_Web_Authentica tion	0					
	Compliance_Unknown_Devices	Ø			+ New AND OR		
	Compliant_Devices	Ø					
	EAP-MSCHAPv2	0					

Set the Registered-IP-Phone rule to Pica8-dynamic-voice-VLAN Authorization profile as shown below. Click Save.

Image: Set of the state of	Status	Policy Set Name	Description	Conditions		CILK THEFE ID I	to writeless setup and visionity setup	DO NOT BROM	r une ag				
Adda	erch 🥥	Pica8-Mab-Auth		Uvred_MAB			Default Network Access	× ×	+				
Status Rest Name Condition Los Meters Status Status <td colspan="4" sta<="" th=""><th>Authenticati</th><th>on Policy (2)</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></td>	<th>Authenticati</th> <th>on Policy (2)</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>				Authenticati	on Policy (2)							
implicit to the series of t	+ Statu	s Rule Name	Conditions			Use	>	Hit	s A				
Image: State Rule Name Conditions artic Result	arch	Pica8-Guest-rule	Wred_MAB			G 3	Jest_Portal_Sequence ×	* 15	1				
O Default If User not found	_					101 x	emal Endpoints × Options Auth fail REJECT ×						
weborization Petroy - Local Exceptions weborization Petroy - Global Exception	0	Default					User not found REJECT # *	•					
Authorization Policy - Local Exceptions Authorization Policy - Global Exceptions Authorization Policy - Global Exceptions Authorization Policy - Global Exceptions Results Results Results Here Here <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>JROP * *</td> <td></td> <td></td>							JROP * *						
Automatation Pails - Giosal Exceptions Automatation Pails - Giosal Exceptions Status Rule Name Conditions Rule Name Conditions Results earch	Authorizatio	n Policy - Local Exceptions											
Status Rule Name Conditions Results * Status Rule Name Profiles Security Groups Hits	Authorizatio	n Policy - Global Exceptions											
Status Rule Name Conditions Polles Security Groups Hits	sumonizatio	Policy (5)											
anh	+ Statu	s Rule Name	Conditions		Results Profiles	Sec	urity Groups	Hit	s A				
	earch												

Verifying the NAC Configuration

Connect the IP Phone to port ge-1/1/5.

On the PicOS switch, run the following CLIs to verify the MAB Authentication for the IP Phone.

Client MAC	: 00:c1:b1:e5:0a:f6
Status	: authorized
Success Auth Method	: MAB
Last Success Time	: Wed Oct 13 13:31:53 2021
Traffic Class	: Voice
Dynamic VLAN ID	: 800 (active)



When Employee laptop with 802.1x supplicant is connected behind an IP phone, following is the output:

admin@P8-Access-BR-1-SW-2> show dot1x interface gigabit-ethernet ge-1/1/5

Interface ge-1/1/5:

Client MAC	: 00:c1:b1:e5:0a:f6
Status	: authorized
Success Auth Method	: MAB
Last Success Time	: Wed Oct 13 13:31:53 2021
Traffic Class	: Voice
Dynamic VLAN ID	: 800 (active)
Client MAC	: 80:e8:2c:b9:28:db
Client MAC Status	: 80:e8:2c:b9:28:db : authorized
Client MAC Status Success Auth Method	: 80:e8:2c:b9:28:db : authorized : Dotlx
Client MAC Status Success Auth Method Last Success Time	: 80:e8:2c:b9:28:db : authorized : Dot1x : Wed Oct 13 13:45:06 2021
Client MAC Status Success Auth Method Last Success Time Traffic Class	: 80:e8:2c:b9:28:db : authorized : Dot1x : Wed Oct 13 13:45:06 2021 : Other
Client MAC Status Success Auth Method Last Success Time Traffic Class Dynamic VLAN ID	: 80:e8:2c:b9:28:db : authorized : Dotlx : Wed Oct 13 13:45:06 2021 : Other : 10 (active)
Client MAC Status Success Auth Method Last Success Time Traffic Class Dynamic VLAN ID Dynamic Filter Name	: 80:e8:2c:b9:28:db : authorized : Dot1x : Wed Oct 13 13:45:06 2021 : Other : 10 (active) : mac_auth_policy_2 (active)

To view a real-time authentication summary navigate to *Operations->RADIUS->Live Logs* and click on the icon under the *Details* column as shown below.

ahaha Id	entity Services	Engine H	Home Context Visibility	✓ Operation	s Policy Administration	Work Centers		License Warr	ning 🔺 🔍
- RADIL	IS Threat-Cent	tric NAC Live Log	gs + TACACS + Trouble	eshoot + Adapt	tive Network Control Reports			Click here to do wireless setup and visit	pility setup Do not s
Live Log	s Live Session	s							
		Misconfigu	red Supplicants	Misconfigured	Network Devices 🕲	RADIUS Drops	Client Stopped Responding	Repeat Counter)
			0		0	0	0	14	
			-		-	-	-		
							Refresh Never	~ Show Latest 100 records	V Within Last
C Refr	esh O Reset	Repeat Counts	A Export To 🗸						,
Details	Repeat	Identity	Endpoint ID	Endpoint	Authentication Policy	Authorization Policy	Authorization Pr	ofiles	Device Port
		Identity	Endpoint ID	Endpoint Pn	Authentication Policy	Authorization Policy	Authorization Pro	files	Device Port
ò	1	jdoe	80:E8:2C:B9:28:DB	HP-Device	Pica8-Employee >> Default	Pica8-Employee >> Default	pica8-employee-a	cl-profile,pica8-employee-vlan-profile	
ò		jdoe	80:E8:2C:B9:28:DB	HP-Device	Pica8-Employee >> Default	Pica8-Employee >> Default	pica8-employee-a	cl-profile,pica8-employee-vlan-profile	
ò	4	00:C1:	00:C1:B1:E5:0A:F6	Cisco-Device	Pica8-Mab-Auth >> Pica8-Gues	Pica8-Mab-Auth >> Registered-IP-Pho	ne pica8-dynamic-voi	ce-vlan	

Overview							
Event	5200 Authentication succeeded						
Username	00:C1:B1:E5:0A:F6						
Endpoint Id	00:C1:B1:E5:0A:F6 🕀						
Endpoint Profile	Cisco-Device						
Authentication Policy	Pica8-Mab-Auth >> Pica8-Guest-rule						
Authorization Policy	Pica8-Mab-Auth >> Registered-IP-Phone						
Authorization Result	pica8-dynamic-voice-vlan						



Access Point Authentication

Access Point is connected to port ge-1/1/6 and authenticated using MAB.

Configuring the MAB Wired Access Policy in ISE for an Access Point

Configuring the MAB Wired Access policy in ISE for Access Point involves following four steps:

- 1. Create an Endpoint Identity Group for Access Points and add the Access Point Mac addresses.
- 2. Create an Authorization Profile to dynamically assign VLAN 10 for the Access Points.
- 3. Create an Authorization Profile to use downloadable ACL mac_auth_policy_3 configured in ISE.
- 4. Create a Wired Access policy for Access Points that will use the above two authorization profiles.

Create an Endpoint Identity Group for Access Points and add Access Point Mac Addresses

To create AP-Group Endpoint Identity Group, navigate to Administration -> Identity Management -> Groups -> Endpoint Identity Groups->Registered Devices and click + as shown below.

Home Home Home	Context Visibility Operations	Policy Acministration Work Centers
System Identity Management Network	tesources + Device Portal Management	pxGrid Services
Identities Groups External Identity Sources	Identity Source Sequences + Settings	
Identity Groups	Endpoint Identity Groups	
(۵, ۲		
4 · E · 8.	/ Edit -444 XDelete	
Endpoint Identity Groups	Name	Description
 User Identity Groups 	Android	Identity Group for Profile: Android
	Apple IDevice	Identity Group for Profile: Apple-IDevice
	Avis-Device	Identity Group for Profile: Axis-Device
	BlackBerry	Identity Group for Profile: BlackBerry
	I Backlist	Blacklist Identity Group
	Gisco-IP-Phone	Identity Group for Profile: Clsco-IP-Phone
	Cisco-Meraki-Device	Identity Group for Profile: Cisco-Meraki-Device
	DownloadsbleACLMA8	DownloadabiaACLMAB
	Epecn-Device	Identity Group for Profile: Epson-Device
	GuestEndpoints	Guest Endpoints Identity Group
	IP-Phone	Claco IP Phone
	Juniper-Device	Identity Group for Profile: Juniper-Device
	Profiled	Profiled Identity Group
	Registered Devices	Asset Registered Endpoints Identity Group
	Gony Device	Identity Group for Profile: Sony-Device
	Synology-Device	Identity Group for Profile: Synology-Device
	Trenchel-Device	Identity Group for Profile: Trendnet-Device
	Unknown	Unknown Jdentity Group
	U Vizio-Device	Identity Group for Profile: Vido-Device
	LI Workstation	acentity Group for Profile: Workstation

Enter *Name and Description* and click *Submit*. Select *AP-Group Endpoint Identity Groups* and click *+* and select the MAC address of the Access Point to add MAC address of Access Point as shown below.

-shult- esce Identity Services Engine Home +	Context Visibility Operations	Policy Administration	* Work Centers					
Network Access Guest Access TrustSec	BYOD Profiler Posture	Device Administration + Passiv	Clev					
Overview + Identities Identity Groups Ext Id S	ources + Administration Network De	vices	Manage Accounts	ments Policy Sets	Reports Custom Portal Files	 Settings 		
Identity Groups	Endpoint Identity Group List > AP-Group							
·	* Name AP-Group							
Endpoint identity Groups E Profied Blacklist	Description Parent Group RegisteredDevices			lli.				
Euclide Endpoints Endpoints Endpoints Endpoints Pical-Cisco-IP-Phone	Save Reset							Selected 0 Total 1 😵 🎡 🖕
H AP-Group	Add XRemove +						Show All	- 10
🚠 Unknown	MAC Address	Static Group Assignment	EndPoint Profile					
 User rommy citudes 	38:17:C3:C0:A1:68	true	HP-Device					

Create an Authorization Profile to Dynamically Assign a VLAN for Access Points

To create the Authorization Profile, navigate to *Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles* and click + as shown below.



cisco Identity Services Engine	Home + Context Visibility + Operations	Policy Administration Work Centers	Lionon Warning 🔺 🔍 💿 🔹
Policy Sets Profiling Posture Cl	ent Provisioning Policy Elements		
Dictionative + Conditions + Result	e		
9			
Authentication Authorization	Standard Authorization Profiles For Policy Export go to Administration > Syst	em > Backup & Rostore > Policy Export Page	Salesse Ó Tour 11 🏀 🎯 🕳
Authorization Profiles	/ Inder of Ander 25 Duplication 🗙 Derivation		Show All - 15
Developitable ACLe	Name Name	Frofie	Description
Downloadable Moca	 Generic Geest Access 	- PCOS 🕀	
+ Profiling	PicaB-Vian10	PICOS (II)	Assigns Vian 10 to Pica8 EMployees
+ Posture	pice8-vian-aci-profile	PCOS 🕀	
	Blackhole_Wireless_Access	ath Citate (1)	Default profile used to blacklist wheleas devices. Ensure that you configure a BLACKHOLE AGL on the V
Glient Provisioning	Cisco_IP_Phones	at Citco 🗉	Default profile used for Cloco Phones.
	Cisco_Temporal_Onboard	at Cisco 🕀	Onboard the device with Gisco temporal agent
	Cisco_WebAuth	at Clean ()	Default Profile used to recirect users to the CWA portal.
	NSP_Orboard	25 Ckoo 🕀	Onboard the device with Native Supplicant Provisioning
	Non Caso IP Phones	at Caro D	Debuil Profile used for Non Class Phones.
	Dere-Access		Default Profile with access type as Access-Reject
	PermitAccess		Debuil Profile with access type as Access-Accept

Enter *Name, Description*, set *Access Type to ACCESS_ACCEPT*, and set *Network Device Profile* to *PicOS*. Check the box for *VLAN* and enter an attribute value that identifies a VLAN. In this example VLAN ID 10 is used. Click *Submit*.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Cli	ient Provisioning V Policy Elements
Dictionaries > Conditions Results	
0	
Authentication	Authorization Profiles > Pica8-mab-vlan-profile
	Authorization Profile
- Authorization	* Name Pica8-mab-vian-profile
Authorization Profiles	Description
Downloadable ACLs	* Access Type ACCESS_ACCEPT T
▶ Profiling	Network Device Profile 🔀 PICOS + 🕀
Posture	
Client Provisioning	
	▼ Common Tasks
	Security Group
	- • •
	VLAN Tag ID 1 Edit Tag IDIName 10
	 Advanced Attributes Settings
	Select an item 💿 = 💿 — 🕂
	* Attributes Details
	Access Type = ACCESS ACCEPT
	Turnel-Private-Group-ID = 1:10 Turnel-Type = 1:13
	Tunnel-Medium-Type = 1:6
	Save Reset

In the above example we have added Pica8-mab-VLAN-profile for dynamically assigning a VLAN for Access Points.

Create Authorization Profile to Use Downloadable ACL mac_auth_policy_3 Configured in ISE

To create the Authorization Profile, navigate to Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles and click + as shown below.

Enter *Name* as *Pica8-Downloadable-ACL, Description*, set Access Type to *ACCESS_ACCEPT*, then set the *Network Device Profile* to *PicOS* as shown below. Expand *Advanced Attribute Settings* and set the attributes shown below to download ACL from ISE:

• Select Pica8:Pica8-IP-Downloadable-ACL-Name attribute and set man_auth_policy_3 as value.

· Select Pica8:Pica8-IP- Downloadable-ACL-Rule and set the rules as shown below. Click Submit.

ACL rules only permit the endpoint to access a few servers in 192.168.42.0/24 network.



dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Clier	nt Provisioning Policy Elements
Dictionaries Conditions Results	
0	Authorization Profiles > New Authorization Profile
Authentication	Authorization Profile
Authorization	* Name Pica8-downloadable-ACL
Autorization	Description Downloadable ACL for PIcOS
Authorization Profiles	*Access Type ACCESS_ACCEPT T
Downloadable ACLs	Network Device Profile 23 PICOS 👻 🕀
Profiling	
Posture	
Client Provisioning	▼ Common Tasks
	ACL (Filter-ID)
	✓ Advanced Attributes Settings
	Pica8-IP-Downloadable-ACL-Name O = mac_auth_policy_3
	3:Pica8-IP-Downloadable-ACL-Rule 🕥 = 168.42.71/32 then action forward 😒 —
	EPica8-IP-Downloadable-ACL-Rule 💿 = 2.168.42.1/32 then action forward 😒 —
	3:Pica8-IP-Downloadable-ACL-Rule 🚫 = sequence 3 from destination-addr 🚫 —
	3:Pica8-IP-Downloadable-ACL-Rule 💿 = ence 4 from destination-address-i 😒 —
	3:Pica8-IP-Downloadable-ACL-Rule 📀 = nce 5 from destination-address-ic 😒 —
	EPica8-IP-Downloadable-ACL-Rule 💿 = 2.168.42.0/24 then action discard 😒 —
	3:Pica8-IP-Downloadable-ACL-Rule 💿 = sequence 7 then action forward 💿 — 🕂
	▼ Attributes Details
	Access Type = ACCESS_ACCEPT Pica8-IP-Downloadable-ACL-Name = mac_auth_policy_3 Pica8-IP-Downloadable-ACL-Rule = sequence 1 from destination-address-ipv4 192.168.42.71/32 then action forward Pica8-IP-Downloadable-ACL-Rule = sequence 3 from destination-address-ipv4 192.168.42.105/32 then action forward Pica8-IP-Downloadable-ACL-Rule = sequence 3 from destination-address-ipv4 192.168.42.105/32 then action forward Pica8-IP-Downloadable-ACL-Rule = sequence 4 from destination-address-ipv4 192.168.42.105/32 then action forward Pica8-IP-Downloadable-ACL-Rule = sequence 4 from destination-address-ipv4 192.168.42.105/32 then action forward
	Pica8-IP-Downloadable-ACL-Rule = sequence 6 from destination-address-lpv4 192.168.42.0/24 then action discard Pica8-IP-Downloadable-ACL-Rule = sequence 7 then action forward
	<u>y</u>
	Submit Cancel

Please note: ISE and other Radius servers have threshold of 4096 bytes for size of the Access-Accept messages used by the Radius server for DACL. If your ACL size is huge, you will run into problems. For this purpose PicOS uses abbreviated downloadable ACLs. Please refer to the Downloadable ACL section in the documentation page.

Create a Wired Access Policy for the Access Point

Let us create a new rule in the *Policy Set called Pica8-Mab-Auth* to authenticate the Access Point, place it on VLAN 10, and use the downloadable ACL we have set up in the earlier step. Navigate to *Policy -> Policy Sets* and click > on the *Pica8-Mab-Auth* policy we previously created as shown below.

Create a new rule under Authorization Policy called Registered-Device-Rule. Click the + sign under Conditions. Select Endpoint Identity Groups:Registered Devices: AP-Group for Conditions as shown below and click Save. Set the Authorization Policy for this rule to Pica8-Downloadable-ACL and Pica8-mab-VLAN-profile as shown below. Click Save.



dindin Id	entity Ser	vices Engine Home 🕠	Context V	sibility Operations	* Polic	y Administration	n →V	Work Centers	5									License Wa	iming 🔺 🤉 9	. 0	• •												
Policy S	ets Profi	ling Posture Client Provisionin	g ≯Po	licy Elements	_											Click h	ere to do wirek	ess setup and vi	sibility setup Do	not show I	his again. $ imes$												
Policy	Sets →	Pica8-Mab-Auth															Rese	t Policyset H	itcounts	Reset	Save												
	Status Policy Set Name Description Conditions Allowed Protocols / Server Sequence Hits																																
Search	and Landau a																																
	0	Pica8-Mab-Auth				Wired_MAB												Default Netw	ork Access	x * ·	+ 336												
❤ Auth	Authentication Policy (2)																																
+	Status	Rule Name	Cond	itions													Use			Hits	Actions												
Searc	h																																
	Ø	Pica8-Guest-rule	8	Wired MAB													Guest_Po	rtal_Sequence	x *	170	0												
																_	> Option	ns															
																	Internal Er	ndpoints	х т														
																	✓ Option	ns															
																	If Auth fai																
	\odot	Default															REJECT		× *	0	0												
																	If User no	it found															
																REJECT	× *																
																													If Process	s fail			
																	DROP		х т														
																	_																
> Auth	orization	Policy - Local Exceptions																															
> Auth	orization	Policy - Global Exceptions																															
✓ Auth	orization	Policy (5)																															
														Re	sults																		
+	Status	Rule Name	Cond	itions										Pr	ofiles		Security G	iroups		Hits	Actions												
Searc	h																																
_	Ø	Registered-IP-Phone	48	IdentityGroup-Name EQU	IALS End	dpoint Identity Groups:F	Registered	redDevices:Pic	ca8-Cisco-IP-	P-Phone				0	× pica8-dynamic-voice-vlan	+	Select from	m list	- +	0	٥												
1	ø	Registered-Device-Rule	48-	IdentityGroup-Name EQU	IALS End	dpoint Identity Groups:F	Registered	edDevices:AP-	P-Group					0	× Pica8-downloadable-ACL × Pica8-mab-vlan-profile	+	Select from	m list	- +	166	٥												
	ø	Pica8-known-guests	48-	IdentityGroup-Name EQU	IALS End	dpoint Identity Groups:0	GuestEnd;	ndpoints:Self_R	Register_Gu	uest				8	× Pica8-Guest-ACL × Pica8-guest-VLAN	+	Select from	n list	- +	0	٥												
	Ø	Pica8-unknown-guests	48	IdentityGroup-Name NOT	_EQUAL	S Endpoint Identity Gr	roups:Gue	uestEndpoints:	::Self_Registe	ter_Guest					× CWA_preauth	+	Select from	n list	- +	4	٥												
	Ø	Default													× DenyAccess	+	Select from	n list	- +	0	٥												
																			(Reset	Save												

Verifying the NAC Configuration

On the PicOS switch run the following CLI to verify the MAC RADIUS authentication. admin@P8-Access-BR-1-SW-2> show dot1x interface gigabit-ethernet ge-1/1/6 Interface ge-1/1/6:

Client MAC	: 38:17:c3:c0:a1:68
Status	: authorized
Success Auth Method	: MAB
Last Success Time	: Tue Oct 26 11:25:34 2021
Traffic Class	: Other
Dynamic VLAN ID	: 10 (active)
Downloadable Filter Name	: mac_auth_policy_3 (active)
Downloadable Filter Rule	: sequence 1 from destination-address-ipv4 192.168.42.71/32
	sequence 1 then action forward
	<pre>sequence 2 from destination-address-ipv4 192.168.42.1/32</pre>
	sequence 2 then action forward
	sequence 3 from destination-address-ipv4 192.168.42.105/32
	sequence 3 then action forward
	<pre>sequence 4 from destination-address-ipv4 192.168.42.94/32</pre>
	sequence 4 then action forward
	<pre>sequence 5 from destination-address-ipv4 192.168.42.108/32</pre>
	sequence 5 then action forward
	<pre>sequence 6 from destination-address-ipv4 192.168.42.0/24</pre>
	sequence 6 then action discard
	sequence 7 then action forward



To view a real-time authentication summary navigate to *Operations->RADIUS->Live Logs* and click on the icon under the *Details* column as shown below.

all all a	Martin Bardana Basta										-
cisco	Identity Services Engine	Home Cor	ntext Visibility	 Operations 	Policy Adminis	tration Work Centers					
* R/	ADIUS Threat-Centric NAC Live L	.ogs + TACACS	+ Troublesho	ot + Adaptive	Network Control Report	5				Olick have to do wi	miner 4
Live	Logs Live Sessions									Crick here to do wi	Ciess s
-											
		Misconfigu	red Supplicants	0	Misconfigure	ed Network Devices		RADIUS Drops ()	Client Stopped Responding 0	Repeat Coun	ter
			0			0		0	0	4	
			0			0		0	0	1	
										Refresh Never ~ Show	Latest 1
		-									
0	Refresh O Reset Repeat Count	is 🖉 Export To									
	Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authentication Policy	Authorization Policy	Authorization Profiles	
×					Manthi	Endosint ID	Endooint Profi	Authentication Policy	Authorization Policy	Authorization Profiles	
					- sources	Endpoint to	Lingoine Profi	Parameter	Patron autor (Polog	Parionalisti Pronos	
Ι.	Oct 26, 2021 11:25:18.967 AM	0	0	1	38:17:C3:C0:A1:68	38:17:C3:C0:A1:68	HP-Device	Pica8-Mab-Auth >> Pica8-Guest-rule	Pica8-Mab-Auth >> Registered-Device-Rule	Pica8-downloadable-ACL,Pica8-mab-vlan-pro	file
	Oct 26, 2021 11:25:18.926 AM	2			38:17:C3:C0:A1:68	38:17:C3:C0:A1:68	HP-Device	Pica8-Mab-Auth >> Pica8-Guest-rule	Pica8-Mab-Auth >> Registered-Device-Rule	Pica8-downloadable-ACL,Pica8-mab-vlan-pro	file
	Oct 26, 2021 11:25:18.726 AM	•	ò			38:17:C3:C0:A1:68					_
	Ort 26, 2021 11-18-52 004 AM		12		38-17-03-00-41-68	38-17-03-00-61-68	HP. Davice	Diral Mah Auth xx Dirall Guart rule	Dickli Mab. Auth xx Designand Design Dula	Dical downloadable ACI Dical mabulan oro	Ele.
_	Oct 26, 2021 11:18:52:504 AM	<u></u>	-0		38.17.03.00.41.66	36.17.03.00.41.66	HP-Devide	Picalo-Mab-Autri >> Picalo-Guest-rule	Picas-Mab-Aubi >> Registered-Device-Rule	Picas-downloadable-Acc, Picas-mab-vian-pro	110

Overview	
Event	5200 Authentication succeeded
Username	38:17:C3:C0:A1:68
Endpoint Id	38:17:C3:C0:A1:68 ⊕
Endpoint Profile	HP-Device
Authentication Policy	Pica8-Mab-Auth >> Pica8-Guest-rule
Authorization Policy	Pica8-Mab-Auth >> Registered-Device-Rule
Authorization Result	Pica8-downloadable-ACL,Pica8-mab-vlan-profile

Guest Laptop Using Central Web Authentication

In this case, the switch detects that the Mac OS endpoint does not have an 802.1X supplicant. Because MAC RADIUS authentication is also enabled on the interface, the switch then attempts MAC RADIUS authentication for the detected client. We will use Central Web Authentication method for Guest laptops. The guest laptop is connected to port ge-1/1/7.

Logic for Guest laptop with Central Web Authentication is as follows: Guest laptop is not a registered device. Hence it prompts the user to login to the Guest Portal. After user successfully logins to the Guest Portal, dynamic VLAN and ACL are assigned to the port.

This use case involves configuring the PicOS switch, configure the ISE node, and verifying the NAC configuration.

Configuring the PicOS Switch

Configure the Dynamic ACL to be used when a guest laptop connects to a port. This firewall filter, which is configured on the switch, allows the guest to access the entire network except for subnet 192.168.42.0/24.

```
set protocols dot1x filter mac_auth_policy_1 sequence 4 from destination-address-ipv4
192.168.42.170/32
set protocols dot1x filter mac_auth_policy_1 sequence 4 then action "forward"
set protocols dot1x filter mac_auth_policy_1 sequence 5 from destination-address-ipv4
192.168.42.0/24
```



set protocols dot1x filter mac_auth_policy_1 sequence 5 then action "discard"
set protocols dot1x filter mac_auth_policy_1 sequence 6 from destination-address-ipv4
192.168.42.105/32
set protocols dot1x filter mac_auth_policy_1 sequence 6 then action "forward"
set protocols dot1x filter mac auth policy 1 sequence 999 then action "forward"

Configure *Block VLAN*. Guest user will be put in the Block VLAN until the guest user successfully logs into the Guest Portal. Guest laptop will get an IP address in Block VLAN (192.168.44.0/24) before the user logs into the Guest Portal.

set protocols dot1x block-vlan-id 20
set vlans vlan-id 20 vlan-name "vlan20"
set vlans vlan-id 20 13-interface "vlan20"
set 13-interface vlan-interface vlan20 address 192.168.44.1 prefix-length 24

Configuring the ISE Node With a Central Web Authentication Policy

Configuring the Wired Access policy in ISE for guest laptops using Central Web Authentication (CWA) involves following eight steps:

- 1. Create Identity Sequence for the Guest Portal
- 2. Create Guest Type
- 3. Create Self-Registered Guest Portal
- 4. Add a test user with login credentials in the Guest Portal
- 5. Create an Authorization Profile to prompt the user to login to the Guest Portal
- 6. Create an Authorization Profile to dynamically assign VLAN 10 for the guest laptop
- 7. Create an Authorization Profile to dynamically assign an ACL called mac_auth_policy_1. This firewall filter, which is configured on the switch, allows the guest to access the entire network except for subnet 192.168.42.0/24.
- 8. Use General Pica8-Mab-Auth policy set for guest laptop that will use the above three authorization profiles

Create Identity Sequence for the Guest Portal

To create the Guest Portal Identity Sequence , navigate to *Work Centers -> Guest Access -> Identities -> Identity Source* Sequence and click + as shown below.

cisco Identity Services Engine	Home	Operations Policy	y Administration	✓ Work Centers
Network Access Guest Access	TrustSec BYOD Profiler	Posture Device	Administration + Passiv	elD
Overview - Identities dentity Grou	ps Ext Id Sources + Administrati	on Network Devices	Portals & Components	Manage Accounts Policy Elem
0				
Endpoints	Identity Source Sequences	on > System > Backup & I	Restore > Policy Export Pa	00
Network Access Users		on - Oyalam - Daonap a l		9v
dentity Source Sequences	/ Edit 🕂 Ada 🖓 Duplicate 🔰	Collete Collete		
	Name	-	Description	
	All_User_ID_Stores		A built-in Identity Sequent	ce to include all User Identity Stores
	Certificate_Request_Sequence	x0	A built-in Identity Sequent	ce for Certificate Request APIs
	Guest_Portal_Sequence		A built-in Identity Sequent	ce for the Guest Portal
	MyDevices_Portal_Sequence		A built-in Identity Sequent	ce for the My Devices Portal
	Sponsor_Portal_Sequence		A built-in Identity Sequen	ce for the Sponsor Portal

Enter *Name* of the sequence as *Guest_Portal_Sequence* and select the values for *Authentication Search List* as shown below and click *Save*.



cisco	Identity Ser	vices Engine	Home >	Context Visibility	 Operations 	Policy	 Administration 	- Work Centers	
► Net	work Access	▼ Guest Access	 TrustSec 	BYOD Profile	er I Posture	Device Add	ministration	velD	
Overv	iew 👻 Identi	ties Identity Grou	ps Ext Id So	urces + Administr	ation Network	Devices +	Portals & Components	Manage Accounts	 Policy Ele
		G	Identity Sou	rce Sequences List >	Guest_Portal_S	Sequence			
Endpoin	its		Identity :	source sequenc	e				
Network	Access Users		* Identi	cy Source Sequei	ice				
Identity	Source Seque	nces	* Nar	me Guest_Portal_S	equence				
			Descripti	on A built-in Ident	ity Sequence for t	the Guest Porta	al		
									///.
			▼ Certi	ficate Based Auth	hentication				
			[Select Certificate	Authentication Pr	ofile	٣		
			▼ Auth	entication Search	1 List				
				A set of identit	ty sources that wi	ill be accessed	in sequence until first a	authentication succee	ds
			Availa	able			Selected		
			Inter	nal Endpoints			Internal Users		
						>	Guest Users All AD Join Points		$\overline{}$
						<			~
						\gg			\sim
						~			\mathbf{X}
			▼ Adva	nced Search List	Settings				
			If a selec	ted identity store can	not be accessed	for authenticat	ion		
			🔨 🔿 Do	not access other sto	res in the sequen	ce and set the	"AuthenticationStatus"	attribute to "ProcessE	Error"
			 Tre 	at as if the user was	not found and pro	oceed to the ne	ext store in the sequence	e	
			Save	Reset					

Create Guest Type

To create a new *Guest Type*, navigate to *Work Centers -> Guest Access -> Portals & Components-> Guest* Types and click *Create* as shown below.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Network Access Guest Access	TrustSec BYOD Profiler Posture Device Administration PassiveID
Overview + Identities Identity Group	ps Ext Id Sources + Administration Network Devices + Portals & Components Manage Accounts + Policy Elements
Cuest Portals Cuest Types Sponser Groups Sponser Portals	Guest Types You can edit and customize the default guest types and create additional ones. Create Edit Duplicate Delete Contractor (default) Default settings allow network access for up to a year.
	Deliy (default) Default settings allow network access for just 1-6 days. Self_Register_Guest



Enter *Guest Type* name as *Self_Register_Guest* and enter other values shown below including the following: • Enter *Self_Register_Guest* for *Endpoint identity group for guest device registration field*.

• Enter Sponsor Groups as shown below

Click Save.

dentity Services Engine Home	e → Context Visibility →	Operations	
Network Access Guest Access	stSec + BYOD + Profiler	Posture Device Administration PassiveID	Click here to do wirele
Overview Identities Identity Groups	Ext Id Sources Administration	ion Network Devices Portals & Components Manage Accounts Policy Elements Policy Sets Reports Custom Portal Files Set	ttings
Gue	est Type	Save Close	
	Guest type name: *	Self_Register_Guest	
	Description:		
Guest Portale		Language File 👻	
Guest Types			
Sponsor Groups	Collect Additional Data	Custom Helds	
Sponsor Portals	Maximum Access Time		
		Account duration starts	
		From first login From sponsor-specified date (or date of self-registration, if applicable)	
		Maximum account duration	
		5 days v Default 1 (1-999)	
		Allow access only on these days and times:	
		From 9:00 AM To 5:00 PM Sun Mon Tue Wed Thu Fri Sat +	
		Configure quest Account Purge Policy at:	
		Work Centers > Guest Access > Settings > Guest Account Purge Policy	
	Login Options		
		Maximum simultaneous logins 3 (1-999)	
		When guest exceeds limit:	
		ODisconnect the oldest connection ODisconnect the newest connection	
		Redirect user to a portal page showing an error message (i)	
		This requires the creation of an authorization policy rule	
		Maximum devices guests can register: 5 (1-999)	
		Endpoint identity group for guest device registration Self_Register_Guest	
		Configure endpoint identity groups at: Work Centers > Guest Access > Identity Groups	
		The endpoints in this group will be purged according to the policies defined in: Administration > Identity Management > Settings > Endpoint purge	
		Allow guest to bypass the Guest portal	
Ac	ccount Expiration Notification		
		Send account expiration notification 3 days v before account expires (
		View messages in: English - English v	
		Email	
		Send a copy of the notification email to the Sponsor	
		Use customization from: Sponsor Portal (default) v	
		Messages: Copy text from:	
		Your account is going to expire in 3 days. Please notify your sponsor to extend your account now to avoid any delays.	
		Send test email to me at:	
		Send	
		Configure SMTP server at: Work Centers > Guest Access > Administration > SMTP server	
		SMS	
		Messages: Copy text from:	
		Your account is going to expire in 3 days. Please notify your sponsor to extend your account now to avoid any delays.	
		(160 character limit per message*)*Over 160 characters requires multiple messages.	
		Send test SMS to me at: phone number Global Default Send	
		Configure SMS service provider at: Work Centers > Guest Access > Administration > SMS Gateway Providers	
		These appears around an around this quest time:	
	Sponsor Groups	ALL ACCOUNTS (default) GHOUP_ACCOUNTS (default) OWN_ACCOUNTS (default)	



Create Self-Registered Guest Portal

To create the Guest Portal, navigate to *Work Centers -> Guest Access -> Portals & Components -> Guest Portals* and click *Create* as shown below.

Home Identity Services Engine Home	Context Visibility Operations Policy Administration Vork Centers								
Network Access Guest Access TrustSe	ec + BYOD + Profiler + Posture + Device Administration + PassiveID								
Overview + Identities Identity Groups Ext	Id Sources + Administration Network Devices + Portals & Components Manage Accounts + Policy Elements Policy Sets Reports Custom Portal Files								
0									
Guest Portais	est Portals								
Guest Types	WHORS I WIND								
Sponsor Groups	оние оп эле или на рис-челитич роктик турке, или турке, или чел, челекилык, или инклопке ло динек инселет.								
Sponsor Portals	The Durline Date								
	unance bat Dupicare Delete								
	Hotspot Guest Portal (defourt) Guests do not require username and password credentials to access the network, but you can optionally require an access code								
	Authorization setup required								
	Self-Registered Guest Portal (default) Guests may create their own accounts and be assigned a username and password, or use their social login to access the network								
	Used in 2 rules in the Authorization policy								
	Sponsored Guest Portal (default)								
	Sponsors create guest accounts, and guests access the network using their assigned username and password								

Enter *Portal Name* and other parameters as shown below including selecting *Guest_Portal_Sequence* as Authentication method.





Set *Guest Device Registration* Settings as shown below and enter the URL you want to display after successful Guest Portal login as shown below.

dentity Servie	ces Engine	Home	 Context Visibility 	 Operations 	Policy	✓ Administration	- Work Centers		
Network Access	✓ Guest Access	TrustSec	BYOD Pro	filer + Posture	Device	Administration Passiv	velD		
Overview Identiti	ies Identity Grou	ps Ext Id	Sources + Admin	stration Netwo	rk Devices	▼ Portals & Components	Manage Accounts	 Policy Elements 	Policy
Guest Portals Guest Types Sponsor Groups Sponsor Portals	0	•	 Guest Change Par Guest Device Reg Automatically to A message displ Allow guests to You can set the Device information to Configure guest type Work Centers > Guest 	egister guest devi ays to guests when o register devices maximum number of vill be stored in the es at: uest Access > Cor	gs ces they reach th of supported o endpoint iden figure > Gue	e maximum number of suppo devices in the guest type settin tity group specified in the gue ast Types	rted devices. ngs. est type of the user loggin	ng in to this portal.	
		•	BYOD Settings						
		•	Guest Device Cor	npliance Setting	s				
		•	Post-Login Banne	er Page Settings					
		•	VLAN DHCP Relea	ase Page Setting	IS				
		•	Authentication S	uccess Settings					
		,	Once authenticate Originating Authentica URL: http e.g. cisco.com	d, take guest to: URL ① tion Success page ://www.pica8.com	e I Titip://www	Lusco.com			

Add a Test User With Login Credentials in the Guest Portal

Add a test user picatest2 in the Guest Portal as shown below for GuestType_Resiter_Guest user group.



dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
▶ Network Access	TrustSec BYOD Profiler Posture Device Administration PassiveID
Overview - Identities Identity Grou	ps Ext Id Sources Administration Network Devices Portals & Components Manage Accounts Policy Elements
Endpoints	Network Access Users List > picatest2
Network Access Users	✓ Network Access User
Identity Source Sequences	* Name picatest2
	Status Enabled -
	▼ Passwords
	Password Type: Internal Users
	Password Re-Enter Password
	* Login Password Generate 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 2021-12-28 (yyyy-mm-dd)
	✓ User Groups
	GuestType_Self_Register_Guest 📀 — 🕂
	Save Reset

Create an Authorization Profile to Prompt the User to Login to the Guest Portal

To create the Authorization Profile, navigate to *Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles* and click + as shown below.

Enter Name as CWA_preauth, Description, set Access Type to ACCESS_ACCEPT, set Network Device Profile to PicOS as shown below. Check the box for Web Redirection and select Centralized Web Auth with value Self-Registered Guest Portal as shown below. Then click Submit or Save.



dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture	Client Provisioning Policy Elements
Dictionaries + Conditions	ults
(
Authentication	Authorization Profiles > CWA_preauth
- Andred and an	
* Authorization	*Name CWA_preauth
Authorization Profiles	Description
Downloadable ACLs	* Access Type ACCESS_ACCEPT *
Profiling	Network Device Profile RIPICOS V
Posture	
Client Provisioning	
	▼ Common Tasks
	Web Redirection (CWA, MDM, NSP, CPP) ()
	Centralized Web Auth value Self-Registered Guest Portal (d v
	-
	✓ Advanced Attributes Settings
	Select an item 📀 = 💿 — 🕂
	✓ Attributes Details
	Access Type = ACCESS_ACCEPT Pica8-Redirect-URL = https://ip:port/portal/gateway?mac=ClientMacValue&portal=27041710-2e58-11e9-98fb-0050568775a3&action=cwa
	Save Reset

Creating an Authorization Profile to Dynamically Assign VLAN for Guest Laptops

To create a Pica8-guest-VLAN Authorization Profile for guests, navigate to *Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles* and click + as shown below.

cisce Identity Services Engine	Home Context Visibility Operations	Policy Administration Work Centers	License Warring 📥 🔍 📵 💿 🕸
Policy Sets Profiling Posture (Client Provisioning Policy Elements		
Dictionaries + Conditions - Resu	its		
	•		
Authentication Authorization	Standard Authorization Profiles For Policy Export go to Administration > Syst	am > Backup & Restore > Policy Export Page	Selstood 0 Total 11 😵 🔯 🕳
Authorization Profiles	/ Edit 🕂 🚧 🖓 Duplicate 🗙 Delete		Show All 🛛 👻
Rousioadable ACLs	Name	Profile	Description
Control Color	Generic Guest Access	PICOS 🕀	
Profiling	Pica8-Vlan10	PICOS (1)	Assigns Vian 10 to Pica8 EMployees
> Posture	pica8-vian-aci-profile	PICOS (1)	
	Blackhole_Wireless_Access	👬 Cisco 🕀	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on the V
Client Provisioning	Cisco_IP_Phones	🗰 Cisco 😐	Default profile used for Cisco Phones.
	Gisco_Temporal_Onboard	🗰 Cisco 🕀	Onboard the device with Claco temporal agent
	Cisco_WebAuth	🗱 Cisco 回	Default Profile used to redirect users to the CWA portal.
	NSP_Onboard	🗱 Cisco 💿	Onboard the device with Native Supplicant Provisioning
	Non_Claco_IP_Phones	🟥 Cisco Θ	Default Profile used for Non Olsco Phones.
	DenyAccess		Default Profile with access type as Access-Reject
	PermitAccess		Default Profile with access type as Access-Accept

Enter Name as Pica8-guest-VLAN, Description, set Access Type to ACCESS_ACCEPT, set Network Device Profile to PicOS as shown below. Check the box for VLAN and enter 10 as value as shown below. Then click Submit.



dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Cli	ent Provisioning Policy Elements
Dictionaries	
9	
▶ Authentication	Authorization Profiles > Pica8-guest-VLAN
	Authorization Profile
✓ Authorization	* Name Pica8-guest-VLAN
Authorization Profiles	Description //
Downloadable ACLs	* Access Type ACCESS_ACCEPT *
→ Profiling	Network Device Profile ROM PICOS - O
Client Provisioning	
	Common Tasks
	Security Group
	VLAN Tag ID 1 Edit Tag ID/Name 10
	Web Redirection (CWA, MDM, NSP, CPP) ()
	 Advanced Attributes Settings
	Select an item 📀 = 📀 — 🕂
	- Attributes Details
	Tunnel-Private-Group-ID = 1:10 Tunnel-Type = 1:13 Tunnel-Medium-Type = 1:6

Creating an Authorization Profile to Dynamically Assign an ACL for Guest Laptops

To create a MAB Authorization Profile for guests navigate to *Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles* and click + as shown below.

cisco Identity Services Engine	Home + Context Visibility + Oper	ations Policy + Administration + Work Centers		🛛 Liocnae Warning 🔺 🔍	. 8 0 0
Policy Sets Profiling Posture Clien	Policy Elements				
Dictionaries					
0					
> Authentication	Standard Authorization Profil	85			
	For Policy Export go to Administration	> System > Backup & Restore > Policy Export Page			A 10
+ Authorization	And share Departments Ma	-heter		Scioloc	- 199 -
Authorization Profiles	Vent There all others to	0	Description .	SIDW M	· 10
Downloadable ACLs	Name	Prote	 Description 		
> Profiling	Biese Manual 0	E BICOS @	Assists May 10 to Diard Elifeiruson		
	- Mais-Vianto	E PROS &	Assigns wan to to Prose Employees		
Posture	pics8-vien-ed-profile	PICOS 🕀			
	Blackhole_Wireless_Access	dia Cisco 🕀	Default profile used to blacklist wireless devices. I	Ensure that you configure a BLA	CKHOLE ACL on the V
Client Provisioning	Cisco_IP_Phones	atta Cisco 🕀	Default profile used for Cisco Phones.		
	Cisco_Temporal_Onboard	dia Cisco 🕀	Onboard the device with Cisco temporal agent		
	Cisco_WebAuth	🟥 Cisco 🕀	Default Profile used to redirect users to the CWA	portal.	
	NSP_Onboard	🚓 Cieco 🕀	Onboard the device with Native Supplicant Provis	ioning	
	Non_Cisco_IP_Phones	dia Cisco 🕀	Default Profile used for Non Cisco Phones.		
	 DenyAccess 		Default Profile with access type as Access-Reject		
	PermitAccess		Default Profile with access type as Access-Accept	4	



Enter Name as *Pica8-Guest-ACL, Description*, set *Access Type to ACCESS_ACCEPT*, and set *Network Device Profile* to *PicOS* as shown below. Check the box for *ACL* and enter *mac_auth_policy_1* as value. Click *Submit*.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Cli	ent Provisioning V Policy Elements
Dictionaries + Conditions - Results	
0	
Authentication	Authorization Profiles > Pica8-Guest-ACL
	Authorization Profile
- Authorization	* Name Pica8-Guest-ACL
Authorization Profiles	Description
Downloadable ACLs	* Access Type ACCESS_ACCEPT *
▶ Profiling	Network Davies Profile 111 DICOS - 1
→ Posture	
Client Provisioning	
	Common Tasks
	ACL (Filter-ID) mac_auth_policy_1
	Security Group
	★ Advanced Attributes Settings
	Select an Item 📀 = 📀 — 🕂
	✓ Attributes Details
	Access Type = ACCESS_ACCEPT Filter-ID = mac_auth_policy_1

Use General Pica8-Mab-Auth Policy Set for Guest Laptop

Let us use the previously created Policy Set called Pica8-Mab-Auth to authenticate guests by using Central Web Authentication method. Navigate to *Policy -> Policy Sets* and click > on the *Pica8-Mab_Auth* policy we have previously created and sign in as shown below.

dhihi cisco	Identity Se	ervices Engine Home	Context Visibility	+ Polic	Administration	Work Centers	License Warning 🔺	્	Θ	o o
Polic	Sets Pro	ofiling Posture Client Provisionin	ng				Click here to do wireless setup and visibility se	tup <mark>Do n</mark>	ot show this	again. ×
Polic	y Sets						Reset Policyset Hitcount	s	Reset	Save
+	Status	Policy Set Name	Description	Conditi	ons		Allowed Protocols / Server Sequence	Hits	Actions	View
Sear	ch									
	\odot	Pica8-Mab-Auth			Wired_MAB		Default Network Access × * +	571	٥	>
	\odot	Pica8-Employee			Wired_802.1X		Default Network Access × - +	31	٥	>

Add the following policies as shown below:

- Create Pica8-Guest-rule Authentication policy using Wired-MAB and Guest_Portal_Sequence with the options shown below.
- Create Pica8-unknown-guest Authorization policy as shown below to prompt the user to login to the Guest Portal.
- Create Pica8-known-guest Authorization policy as shown to assign VLAN 10 and dynamically assign an ACL called mac_ auth_policy_1 for guest laptop after guest logs successfully into the Guest profile.

Click Save.



diala cisco	Identity	Service	es Engine Home → C	ontext Vis	ibility	- Policy	Administration	Work Centers				License Warning	۹ م	0	• •
Policy	y Sets	Profiling	Posture Client Provisioning	▶ Poli	cy Elements						Click here	to do wireless setup and visibility	setup <mark>Do n</mark>	ot show th	is again. ×
Polic	y Sets	→ Pic	a8-Mab-Auth									Reset Policyset Hitcou	nts	Reset	Save
	Statu	us Pol	licy Set Name	Descript	lion	Condition	S					Allowed Protocols	Server S	Sequence	e Hits
Sean	°ch ©	Pici	a8-Mab-Auth			C Wi	red_MAB					Default Network Act	055	x - 4	658
∨ A	uthentic	ation Po	blicy (2)												
•	Sta	itus R	ule Name	Condit	ions							Use		Hits	Actions
Se	arch														
		Э р	lica8-Guest-rule	P	Wired MAB							Internal Endpoints	x *	304	ö
			1010-010511010	-	11100_1010							> Options			Ť
		2 5	ha fau di									Internal Endpoints	* *		~
		9 0	erauit									> Options		U	¥
> A	uthoriza	tion Poli	cy - Local Exceptions												
> A	uthoriza	tion Poli	icy - Global Exceptions												
∨ A	uthoriza	tion Poli	icy (5)												
									Re	esults					
+	Sta	itus R	tule Name	Condit	ions				Pr	ofiles	1	Security Groups		Hits	Actions
Se	arch														
_	(N N	anietarad_ID_Phone	.40.	Identitu@mun-Name EO	IIAI 9 Endoni	nt Identitu Omune-Reni	etaradNauinae-DinaR_Cienn_ID_Dhnna	6	× nica8-dvnamic-vnice-vlan	+	Select from list	- +	49	ð
	(R	tegistered-Device-Rule	48.	IdentityGroup-Name EQ	UALS Endpoi	nt Identity Groups:Regi	steredDevices:AP-Group		× Pica8-downloadable-ACL × Pica8-mab-vlan-profile	+	Select from list	• +	81	٥
	(Э Р	lica8-known-guests	盡	IdentityGroup-Name EQ	UALS Endpoi	nt Identity Groups:Gue	stEndpoints:Self_Register_Guest		× Pica8-Guest-ACL × Pica8-guest-VLAN	+	Select from list	• +	114	٥
	(Э Р	lica8-unknown-guests	48.	IdentityGroup-Name NO	T_EQUALS E	ndpoint Identity Groups	s:GuestEndpoints:Self_Register_Gues	t I	× CWA_preauth	+	Select from list	• +	67	٥
	(∂ D	Pefault							× DenyAccess	+	Select from list	• +	0	¢

Verifying the NAC Configuration

Following verification steps are done when guest laptop is connected to port ge-1/1/7.

1. On the PicOS switch run the following CLI to verify the authentication after guest laptop is connected to port ge-1/1/7.

At the beginning you will see guest user laptop is unauthorized.

Then guest user types in https://www.example.com in the Browser running in the laptop.

You can see Guest Registration portal URL is presented to the Endpoint Browser. On the PicOS switch run the following CLI to verify.



admin@P8-Access-BR-1-SW-2# run show dot1x interface gigabit-ethernet ge-1/1/7
Interface ge-1/1/7:

Client MAC	: 80:e8:2c:b9:28:db
Status	: unauthorized
Redirect URL	: https://ISE-26-105.pica8.com:8443/portal/gateway?mac=80-E8-2C-B9-28-
DB&portal=27041710-2e58-	11e9-98fb-0050568775a3&action=cwa&token=e7c39b1e4145cbbb51638ab53c125b5f

During this time Block VLAN 20 is assigned to port ge-1/1/7. You can check using the following command.

VLANID	VLAN Name	Tag	Interfaces
1	default	untagged	ge-1/1/1, xe-1/1/1, te-1/1/1, xe-1/1/2, te-1/1/2 ge-1/1/2, te-1/1/3, te-1/1/4, ge-1/1/4, ge-1/1/5 ge-1/1/6, ge-1/1/7, ge-1/1/8, ge-1/1/9, ge-1/1/10 ge-1/1/11, ge-1/1/12, ge-1/1/13, ge-1/1/14, ge-1/1/15 ge-1/1/16, ge-1/1/17, ge-1/1/18, ge-1/1/24, ge-1/1/20 ge-1/1/21, ge-1/1/22, ge-1/1/23, ge-1/1/24, ge-1/1/25 ge-1/1/26, ge-1/1/27, ge-1/1/28, ge-1/1/29, ge-1/1/30 ge-1/1/31, ge-1/1/32, ge-1/1/33, ge-1/1/34, ge-1/1/35 ge-1/1/36, ge-1/1/37, ge-1/1/38, ge-1/1/39, ge-1/1/40 ge-1/1/41, ge-1/1/42, ge-1/1/43, ge-1/1/44, ge-1/1/45 ge-1/1/46, ge-1/1/47, ge-1/1/48
10	default	untagged tagged	ge-1/1/3, ge-1/1/6
20	VLAN20	untagged tagged	ge-1/1/5, ge-1/1/6, ge-1/1/7, ge-1/1/8, ge-1/1/9 ge-1/1/10, ge-1/1/11, ge-1/1/12, ge-1/1/13, ge-1/1/14 ge-1/1/15, ge-1/1/16, ge-1/1/17, ge-1/1/18, ge-1/1/19 ge-1/1/20, ge-1/1/21, ge-1/1/22, ge-1/1/23, ge-1/1/24 ge-1/1/25, ge-1/1/26, ge-1/1/27, ge-1/1/28, ge-1/1/29 ge-1/1/30, ge-1/1/31, ge-1/1/32, ge-1/1/33, ge-1/1/34 ge-1/1/35, ge-1/1/36, ge-1/1/37, ge-1/1/38, ge-1/1/39 ge-1/1/40, ge-1/1/41, ge-1/1/42, ge-1/1/43, ge-1/1/44 ge-1/1/45, ge-1/1/46, ge-1/1/47, ge-1/1/48
40	VLAN40	untagged tagged	
800	default	untagged Tagged	

admin@P8-Access-BR-1-SW-2# run show vlans

On ISE navigate to **Operations->RADIUS->Live Logs** and click on the icon under the **Details** column as shown below. You can see **Pica8-unknown-guests** authorization policy is triggered. This rule is used for authenticating the guest user whose laptop will not have 802.1x supplicant.



cisco le	dentity Services E	ingine Ho	me + Conte	ext Visibility	- Operations	Policy Admini	istration	Work Centers					License Warn	ing 🔺
* RADI	US Threat-Centri	c NAC Live Logs	+ TACACS	Troubleshoot	 Adaptive Ne 	stwork Control Repo	rts					Click here to do win	eless setup and visib	ility setup D
Live Lo	gs Live Sessions													
		Misco	onfigured Suppl	icants 🛈	Misco	infigured Network Dev	vicos 🛈		RADIUS Drops ()	Client Stoppe	d Responding 🕲	Reper	t Counter 🕘	entication n
			0			0			4749		0		0	rork device :
											Refresh Neuer	Show I	atast 100 records	- Within
											Renear	- 3.04		- main
C Ref	resh O Reset F	Repeat Counts	Export To •											
1	Time	Status		Details	Repeat	Identity	En	dpoint ID Au	uthentication Policy	Authorization Pol	icy	Authorization Profi	Identity Group	Post
×				×		00:80:8e:8a:92:76	×							
,	Nov 04, 2021 04:05:	43	0	a	0	00:80:8E:8A:92:76	00:	:80:8E:8A Pi	ca8-Mab-Auth >> Pica8-Guest-rule	Pica8-Mab-Auth >>	Pica8-unknown-guests	CWA_preauth		
,	Nov 04, 2021 04:05:-	43		Q		00:80:8E:8A:92:76	00:	:80:8E:8A Pi	ca8-Mab-Auth >> Pica8-Guest-rule	Pica8-Mab-Auth >>	Pica8-unknown-guests	CWA_preauth		

Clicking the icon under the Details column opens the *Authentication Detail Report* in a new browser window. This report offers information about authentication status and related attributes, and authentication flow.

Dverview		
Event	5200 Authentication succeeded	
Username	00:80:8E:8A:92:76	
Endpoint Id	00:80:8E:8A:92:76 ⊕	
Endpoint Profile		
Authentication Policy	Pica8-Mab-Auth >> Pica8-Guest-rule	
Authorization Policy	Pica8-Mab-Auth >> Pica8-unknown-quests	

On the endpoint, Guest is redirected to the Guest Registration portal as shown below. Guest enters the credentials to login to the Guest Portal.

	ise-26-105.pica8.com	¢	
CISCO Guest Portal			
Welcome Sign on for guest access.			
	Username:		
		t ~	
	Password:		
	Sign On		



After Guest is successfully authorized, run the following CLI on the switch to verify. Here you can see VLAN 10 and *mac_auth_policy_1 ACL* are dynamically assigned to *ge-1/1/7 port*.

admin@P8-Access-BR-1-SW-2> show dot1x interface gigabit-ethernet ge-1/1/7
Interface ge-1/1/5:

Client MAC	: 00:80:8e:8a:92:76
Status	: authorized
Success Auth Method	: MAB
Last Success Time	: Thu Nov 4 16:10:30 2021
Traffic Class	: Other
Dynamic VLAN ID	: 10 (active)
Dynamic Filter Name	: mac_auth_policy_1 (active)

Based on the *Authentication Success Settings* in the *Self-Registered Guest Portal*, guest's laptop browser displays https://www.pica8.com/ page. After this guest will be able to access the Internet.



To verify on ISE, navigate to **Operations->RADIUS->Live Logs** and click on the icon under the **Details** column as shown below.

cisco Ide	ntity Services Engine	Home +	Context Visibility	- Operations	Policy Administra	ation	ня		License War	ning 🔺 🔍 😑 🧿
* RADIU	5 Threat-Centric NAC	Live Logs + TACA	ACS + Troubleshoot	t + Adaptive Net	work Control Reports				Click here to do wireless setup and visi	bility setup Do not show this ag
Live Logs	Live Sessions									
		Misconfigured S	Supplicants ()	Misco	nfigured Network Device	os O	RADIUS Drops ()	Client Stopped Responding ()	Repeat Counter ()	
		C)		0		4816	0	0	
								Refresh Novor	~ Show Latest 100 records	Vithin Last 10 minutes
C Refre	sh 🛛 🗙 Reset Repeat	Counts 🚊 Expo	rt To 🕶							▼ Filter •
Tir	ne	Status	Details	Repeat	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group Por
×			×		Identity	00:80:8e:8a:9 ×	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group Po
No	v 04, 2021 04:10:30	0	0	0	picatest2	00:80:8E:8A	Pica8-Mab-Auth >> Pica8-Guest-rule	Pica8-Mab-Auth >> Pica8-known-guests	Pica8-Guest-ACL,Pica8-guest-VLAN	
No	v 04, 2021 04:10:30		Q		picatest2	00:80:8E:8A	Pica8-Mab-Auth >> Pica8-Guest-rule	Pica8-Mab-Auth >> Pica8-known-guests	Pica8-Guest-ACL,Pica8-guest-VLAN	GuestEndpoints:Self_F

You can see Pica8-known-guests Authorization policy was triggered after Guest successfully logged into the Guest Portal.

Clicking the icon under the Details column opens the *Authentication Detail Report* in a new browser window. This report offers information about authentication status and related attributes, and authentication flow. You can see *Pica8-guest-VLAN* and *Pica8-Guest-ACL* (Dynamic ACL) are assigned to the port where guest laptop is connected.



verview			
Event	5200 Authentication succeeded		
Username	picatest2		
Endpoint Id	00:80:8E:8A:92:76 ⊕		
Endpoint Profile	Unknown		
Authentication Policy	Pica8-Mab-Auth >> Pica8-Guest-rule		
Authorization Policy	Pica8-Mab-Auth >> Pica8-known-guests		
Authorization Result	Pica8-Guest-ACL Pica8-quest-VI AN		
Ithentication Details			
uthentication Details	2021-11-04 16:10:30.2		
uthentication Details Source Timestamp Received Timestamp	2021-11-04 16:10:30.2 2021-11-04 16:10:30.2		
Ithentication Details Source Timestamp Received Timestamp Policy Server	2021-11-04 16:10:30.2 2021-11-04 16:10:30.2 ISE-26-105		
uthentication Details Source Timestamp Received Timestamp Policy Server Event	2021-11-04 16:10:30.2 2021-11-04 16:10:30.2 ISE-26-105 5200 Authentication succeeded		
Ithentication Details Source Timestamp Received Timestamp Policy Server Event Username	2021-11-04 16:10:30.2 2021-11-04 16:10:30.2 2021-11-04 16:10:30.2 ISE-26-105 5200 Authentication succeeded picatest2		
Ithentication Details Source Timestamp Received Timestamp Policy Server Event Username User Type	2021-11-04 16:10:30.2 2021-11-04 16:10:30.2 ISE-26-105 5200 Authentication succeeded picatest2 Host		
uthentication Details Source Timestamp Received Timestamp Policy Server Event Username User Type Endpoint Id	2021-11-04 16:10:30.2 2021-11-04 16:10:30.2 ISE-26-105 5200 Authentication succeeded picatest2 Host 00:80:8E:8A:92:76		
Uthentication Details Source Timestamp Received Timestamp Policy Server Event Username User Type Endpoint Id Calling Station Id	2021-11-04 16:10:30.2 2021-11-04 16:10:30.2 ISE-26-105 5200 Authentication succeeded picatest2 Host 00:80:8E:8A:92:76 00-80-8E-8A-92-76		
Uthentication Details Source Timestamp Received Timestamp Policy Server Event Username User Type Endpoint Id Calling Station Id Endpoint Profile	2021-11-04 16:10:30.2 2021-11-04 16:10:30.2 ISE-26-105 5200 Authentication succeeded picatest2 Host 00:80:8E:8A:92:76 00-80-8E-8A-92-76 Unknown		

Now guest laptop has network access to access the Internet. From the Guest Mac laptop browser make sure you are able to reach www.example.com.

Troubleshooting

This section lists recommended commands for troubleshooting the NAC feature.

Check Whether the ISE Server is Reachable from the PicOS Switch

Verify reachability between ClearPass server and PicOS switch by using the following CLI command:

admin@P8-Access-BR-1-SW-2# run show dot1x server								
Server-IP	Status	Priority	Reti	ry-Interval	Retry-Num	Dete	ect-Interval	Consecutive-Detect-Num
192.168.42.105	active		1	Sec(s)	3	5	Sec(s)	3



Check the NAC Authentication Status of all Ports

Check NAC authentication status for all ports using the following command.

```
admin@P8-Access-BR-1-SW-2> show dot1x interface
Interface 802.1x MAC-RADIUS WEB HOST-MODE CLIENT-MAC CLIENT-STATUS
```

voucput s	uppresse	u				
ge-1/1/5	enable	enable	enable	multiple	00:c1:b1:e5:0a:f6	authorized
					80:e8:2c:b9:28:db	authorized
ge-1/1/6	enable	enable	enable	multiple	38:17:c3:c0:a1:68	authorized
ge-1/1/7	enable	enable	enable	multiple		
ge-1/1/8	enable	enable	enable	multiple		
ge-1/1/9	enable	enable	enable	multiple		

Check the NAC Configuration

<output gunnrogged

To list NAC configuration use the following command.

```
admin@P8-Access-BR-1-SW-2# show all protocols dot1x | display set
    <output suppressed>
set protocols dot1x interface ge-1/1/5 host-mode "multiple"
set protocols dot1x interface ge-1/1/5 auth-mode 802.1x
set protocols dot1x interface ge-1/1/5 auth-mode mac-radius
set protocols dot1x interface ge-1/1/5 auth-mode web
set protocols dot1x interface ge-1/1/5 recovery-timeout 3600
set protocols dot1x interface ge-1/1/5 session-timeout 3600
set protocols dot1x interface ge-1/1/6 host-mode "multiple"
set protocols dot1x interface ge-1/1/6 auth-mode 802.1x
set protocols dot1x interface ge-1/1/6 auth-mode mac-radius
set protocols dot1x interface ge-1/1/6 auth-mode web
set protocols dot1x interface ge-1/1/6 recovery-timeout 3600
set protocols dot1x interface ge-1/1/6 session-timeout 3600
set protocols dot1x interface ge-1/1/7 host-mode "multiple"
set protocols dot1x interface ge-1/1/7 auth-mode 802.1x
set protocols dot1x interface ge-1/1/7 auth-mode mac-radius
set protocols dot1x interface ge-1/1/7 auth-mode web
set protocols dot1x interface ge-1/1/7 recovery-timeout 3600
set protocols dot1x interface ge-1/1/7 session-timeout 3600
set protocols dot1x interface ge-1/1/8 host-mode "multiple"
set protocols dot1x session-timeout 36000
set protocols dot1x block-vlan-id 20
set protocols dotlx aaa radius authentication server-ip 192.168.42.105 shared-key
"cGljYThwaWNhOA=="
set protocols dot1x aaa radius authentication server-ip 192.168.42.105 retry-interval 1
set protocols dot1x aaa radius authentication server-ip 192.168.42.105 retry-num 3
set protocols dot1x aaa radius authentication server-ip 192.168.42.105 detect-interval 5
set protocols dotlx aaa radius authentication server-ip 192.168.42.105 consecutive-detect-num 3
set protocols dot1x aaa radius dynamic-author client 192.168.42.105 shared-key "cGljYThwaWNhOA=="
set protocols dot1x aaa radius nas-ip 192.168.42.170
set protocols dot1x filter mac_auth_policy_1 description ""
set protocols dotlx filter mac auth policy 1 sequence 4 description ""
```



set protocols dot1x filter mac auth policy 1 sequence 4 from destination-address-ipv4 192.168.42.170/32 set protocols dot1x filter mac auth policy 1 sequence 4 then action "forward" set protocols dot1x filter mac auth policy 1 sequence 5 description "" set protocols dot1x filter mac auth policy 1 sequence 5 from destination-address-ipv4 192.168.42.0/24 set protocols dot1x filter mac_auth_policy_1 sequence 5 then action "discard" set protocols dot1x filter mac auth policy 1 sequence 6 description "" set protocols dot1x filter mac auth policy 1 sequence 6 from destination-address-ipv4 192.168.42.105/32 set protocols dot1x filter mac auth policy 1 sequence 6 then action "forward" set protocols dot1x filter mac auth policy 1 sequence 999 description "" set protocols dot1x filter mac auth policy 1 sequence 999 then action "forward" set protocols dot1x filter mac_auth_policy_2 description "" set protocols dot1x filter mac auth policy 2 sequence 999 description "" set protocols dot1x filter mac auth policy 2 sequence 999 then action "forward" set protocols dotlx traceoptions flag configuration disable false

Check VLANs to Verify Dynamic VLANs Assignment to a Port

Check VLANs dynamically assigned for access ports using the following command.

admin@P8-Access-BR-1-SW-2# run show vlans

VLANID	VLAN Name	Tag	Interfaces
1	default	untagged	ge-1/1/1, xe-1/1/1, te-1/1/1, xe-1/1/2, te-1/1/2 ge-1/1/2, te-1/1/3, te-1/1/4, ge-1/1/4, ge-1/1/5 ge-1/1/6, ge-1/1/7, ge-1/1/8, ge-1/1/9, ge-1/1/10 ge-1/1/11, ge-1/1/12, ge-1/1/13, ge-1/1/14, ge-1/1/15 ge-1/1/16, ge-1/1/17, ge-1/1/18, ge-1/1/19, ge-1/1/20 ge-1/1/21, ge-1/1/22, ge-1/1/23, ge-1/1/24, ge-1/1/25 ge-1/1/26, ge-1/1/27, ge-1/1/28, ge-1/1/29, ge-1/1/30 ge-1/1/31, ge-1/1/32, ge-1/1/33, ge-1/1/34, ge-1/1/35 ge-1/1/36, ge-1/1/37, ge-1/1/38, ge-1/1/39, ge-1/1/40 ge-1/1/41, ge-1/1/42, ge-1/1/43, ge-1/1/44, ge-1/1/45 ge-1/1/46, ge-1/1/47, ge-1/1/48
		tagged	
10	default	untagged tagged	ge-1/1/3, ge-1/1/5, ge-1/1/6
20	VLAN20	untagged tagged	ge-1/1/5, ge-1/1/6, ge-1/1/7, ge-1/1/8, ge-1/1/9 ge-1/1/10, ge-1/1/11, ge-1/1/12, ge-1/1/13, ge-1/1/14 ge-1/1/15, ge-1/1/16, ge-1/1/17, ge-1/1/18, ge-1/1/19 ge-1/1/20, ge-1/1/21, ge-1/1/22, ge-1/1/23, ge-1/1/24 ge-1/1/25, ge-1/1/26, ge-1/1/27, ge-1/1/28, ge-1/1/29 ge-1/1/30, ge-1/1/31, ge-1/1/32, ge-1/1/33, ge-1/1/34 ge-1/1/35, ge-1/1/36, ge-1/1/37, ge-1/1/38, ge-1/1/39 ge-1/1/40, ge-1/1/41, ge-1/1/42, ge-1/1/43, ge-1/1/44 ge-1/1/45, ge-1/1/46, ge-1/1/47, ge-1/1/48



40	VLAN40	untagged tagged	
800	default	untagged tagged	ge-1/1/5

Check Dynamic ACL Rules

Check dynamic ACL rules and counters using the following command.

```
admin@P8-Access-BR-1-SW-2> show dot1x dynamic filter
```

Eilton, mag outh no	1
Description	: :
Sequence	: 4
Description	:
Match counter	: 0 packets
Match Condition	: Destination IPv4Net : 192.168.42.170/32
Action	: Forward
Sequence	: 5
Description	:
Match counter	: 0 packets
Match Condition	: Destination IPv4Net : 192.168.42.0/24
Action	: Discard
Sequence	: 6
Description	:
Match counter	: 0 packets
Match Condition	: Destination IPv4Net : 192.168.42.105/32
Action	: Forward
Sequence	: 999
Description	:
Match counter	: 0 packets
Match Condition	:
Action	: Forward
Filter: mac_auth_pol Description	licy_2 :
Sequence	: 999
Description	:
Match counter	: 184547 packets
Match Condition	:
Action	: Forward

Applied Clients : ge-1/1/5 80:e8:2c:b9:28:db



Check Downloadable ACL Rules

Check downloadable ACL rules and counters using the following command.

admin@P8-Access-BR-1-SW-2> show dot1x downloadable filter

Downloadable Filter Name :	mac_auth_	mac_auth_policy_3				
Applied Interface :	ge-1/1/6	ge-1/1/6				
Applied Client MAC :	38:17:c3:	c0:al:	68			
Downloadable Filter Rule :	sequence	1 from	destination-address-ipv4 192.168.42.71/32			
	sequence	1 them	action forward			
	sequence	2 from	destination-address-ipv4 192.168.42.1/32			
	sequence	2 them	action forward			
	sequence	3 from	destination-address-ipv4 192.168.42.105/32			
	sequence	3 them	action forward			
	sequence	4 from	destination-address-ipv4 192.168.42.94/32			
	sequence	4 them	action forward			
	sequence	5 from	destination-address-ipv4 192.168.42.108/32			
	sequence	5 them	action forward			
	sequence	6 from	destination-address-ipv4 192.168.42.0/24			
	sequence	6 them	action discard			
	sequence	7 them	action forward			
Downloadable Rule Counter:	sequence	1	match counter: 1 packets			
	sequence	2	match counter: 0 packets			
	sequence	3	match counter: 0 packets			
	sequence	4	match counter: 0 packets			
	sequence	5	match counter: 0 packets			
	sequence	6	match counter: 0 packets			
	sequence	7	match counter: 903 packets			

Check Trace Logs for Radius

First enable Trace Logs for RADIUS module using the following command: set protocols dot1x traceoptions flag all disable false

Check the Trace Logs for Radius by using the following PicOS command:

```
admin@P8-Access-BR-1-SW-2# run show log last-rows 100 | match DOT1x
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2 local0.debug : [dot1x]
Dmac:80:e8:2c:b9:28:db
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2 local0.debug : [dot1x]
Dmac:80:e8:2c:b9:28:db
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2 local0.debug : [dot1x]
Dmac:80:e8:2c:b9:28:db
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2 local0.debug : [dot1x]send_add_smac_VLAN_port_filter,
mac:80:e8:2c:b9:28:db
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2 local0.debug : [dot1x]Add dynamic filter
rule,ifname:ge-1/1/5 mac 80:e8:2c:b9:28:db
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2 local0.debug : [dot1x]Add dynamic filter
rule,ifname:ge-1/1/5 mac 80:e8:2c:b9:28:db
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2 local0.debug : [dot1x]send add filter,
mac:80:e8:2c:b9:28:db
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2 local0.debug : [dot1x]send add filter,
mac:80:e8:2c:b9:28:db
```



```
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2 local0.debug : [dot1x]rule flag 1, priority 31769
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2 local0.debug : [dot1x]send add filter,
mac:80:e8:2c:b9:28:db
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2 local0.debug : [dot1x]Get transaction id 61377169
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2 local0.debug : [dot1x]Set hw port to dynamic VLAN
cb, ifname:ge-1/1/5 VLAN:10 tid:61377169
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2 local0.debug : [dot1x]Free transaction id 61377169
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2 local0.debug : [dot1x]Mac 80:e8:2c:b9:28:db,VLAN 10,type
dynamic, learn event
Oct 26 2021 15:38:20 P8-Access-BR-1-SW-2 local0.debug : [dot1x]Dmac:00:c1:b1:e5:0a:f6,Smac:18:5a:
58:1d:9c:21
Oct 26 2021 15:39:00 P8-Access-BR-1-SW-2 local0.debug : [dot1x]Get transaction id 62186051
Oct 26 2021 15:39:00 P8-Access-BR-1-SW-2 local0.debug : [dot1x]Free transaction id 62186051
Oct 26 2021 15:46:49 P8-Access-BR-1-SW-2 local0.debug : [dot1x]Mac 00:c1:b1:e5:0a:f6,VLAN 1,type
dynamic, age event
Oct 26 2021 15:46:49 P8-Access-BR-1-SW-2 local0.debug : [dot1x]Mac 80:e8:2c:b9:28:db,VLAN 1,type
dynamic, age event
Oct 26 2021 15:58:24 P8-Access-BR-1-SW-2 local0.debug : [dot1x]Mac 38:17:c3:c0:a1:68,VLAN 1,type
dynamic, learn event
```

Reference

PicOS

The following are reference materials related to PicOS:

- PicOS version 4.1.3 NAC Configuration Guide
- · Configuring Dynamic and Downloadable ACLs for Cisco ISE
- · Abbreviated downloadable ACLs

ISE

The following are reference materials related to Cisco ISE:

- Cisco ISE Installation Guide Release 2.6
- ISE 2.6 Admin Guide
- · Cisco Identity Services Engine Ordering Guide