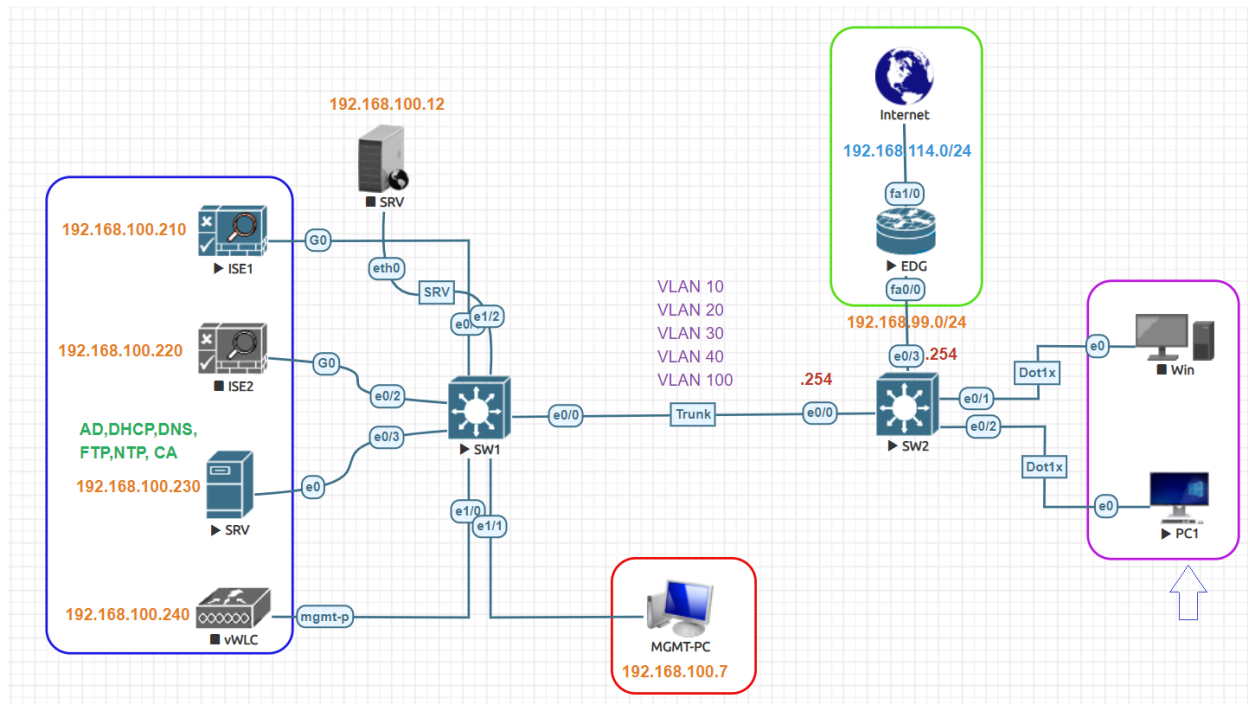


Easy Connect Lab:



Cisco ISE Primary IP Address	192.168.100.210
Cisco ISE Secondary IP Address	192.168.100.220
AD and DNS IP Address	192.168.100.230
CA Server IP Address	192.168.100.230
Domain Name:	test.local
Test User/Group	E1/Employee
Test VLAN	VLAN 20
VLAN Subnet	192.168.20.0/24
VLAN 20 Gateway	192.168.20.1
Authenticator Switch	SW2
Authentication Switch MGMT IP	192.168.100.254
SW2 Dot1x interface	Ethernet 0/2
Computer Hostname	PC1-Win10
Computer Name	PC1

Switch Configuration:

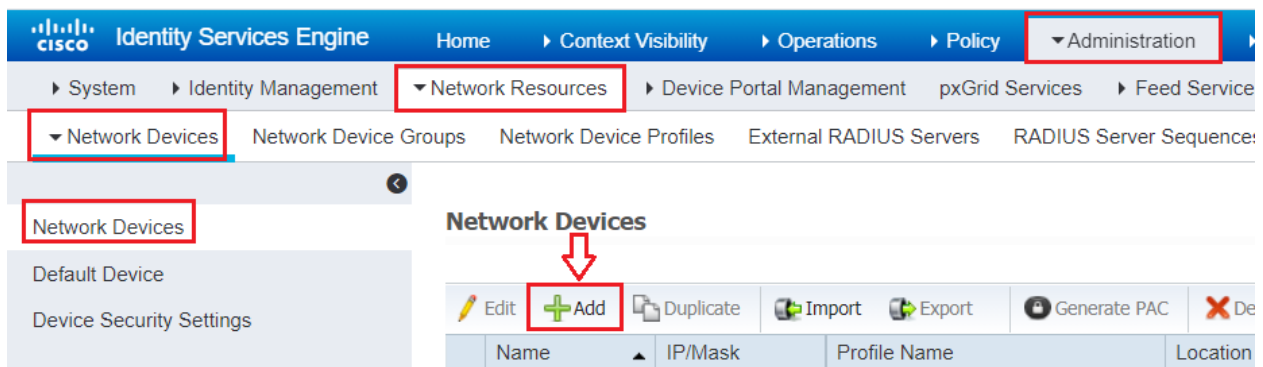
Dot1X Configuration
SW2(config)#aaa new-model
SW2(config)#dot1x system-auth-control
SW2(config)#radius server ISE1
SW2(config-radius-server)# address ipv4 192.168.100.210 auth-port 1812 acct-port 1813
SW2(config-radius-server)#key Test123
SW2(config-radius-server)#radius server ISE2
SW2(config-radius-server)# address ipv4 192.168.100.220 auth-port 1812 acct-port 1813
SW2(config-radius-server)#key Test123
SW2(config-radius-server)#radius-server attribute 6 on-for-login-auth
SW2(config)#radius-server attribute 8 include-in-access-req
SW2(config)#radius-server attribute 25 access-request include
SW2(config)#radius-server vsa send accounting
SW2(config)#radius-server vsa send authentication
SW2(config)#radius-server dead-criteria time 30 tries 3
SW2(config)#radius-server timeout 2
SW2(config)#aaa group server radius ISE-GROUP
SW2(config-sg-radius)#server name ISE1
SW2(config-sg-radius)#server name ISE2
SW2(config-sg-radius)#ip radius source-interface Vlan100
SW2(config-sg-radius)#aaa authentication dot1x default group ISE-GROUP
SW2(config)#aaa authorization network default group ISE-GROUP
SW2(config)#aaa accounting update periodic 5
SW2(config)#aaa accounting dot1x default start-stop group ISE-GROUP
SW2(config)#aaa server radius dynamic-author
SW2(config-locsvr-da-radius)#client 192.168.100.210 server-key Test123
SW2(config-locsvr-da-radius)#client 192.168.100.220 server-key Test123
SW2(config-locsvr-da-radius)#snmp-server community Test123 RO
SW2(config)#interface Ethernet0/1
SW2(config-if)#description win10 node
SW2(config-if)#switchport access vlan 20
SW2(config-if)#switchport mode access
SW2(config-if)#authentication host-mode multi-auth
SW2(config-if)#authentication port-control auto
SW2(config-if)#mab
SW2(config-if)#dot1x pae authenticator
SW2(config-if)#dot1x timeout tx-period 10
SW2(config-if)#spanning-tree portfast edge
SW2(config-if)#authentication event fail action next-method
SW2(config-if)#authentication order dot1x mab

Add Network Device:

Go to **Administration > Network Resources > Network Devices** to add the Device (SW2).



Click on **Add** button to add Network Device like Router and Switch.



Configure **Name** of device, **IP address** configured. Scroll down to set Authentication settings.

The screenshot shows the Cisco Identity Services Engine New Network Device form. The form fields for Name, Description, IP Address, Device Profile, Model Name, Software Version, and Network Device Group are highlighted with red boxes.

Network Devices List > New Network Device

Network Devices

* Name: SW2
Description: SW2

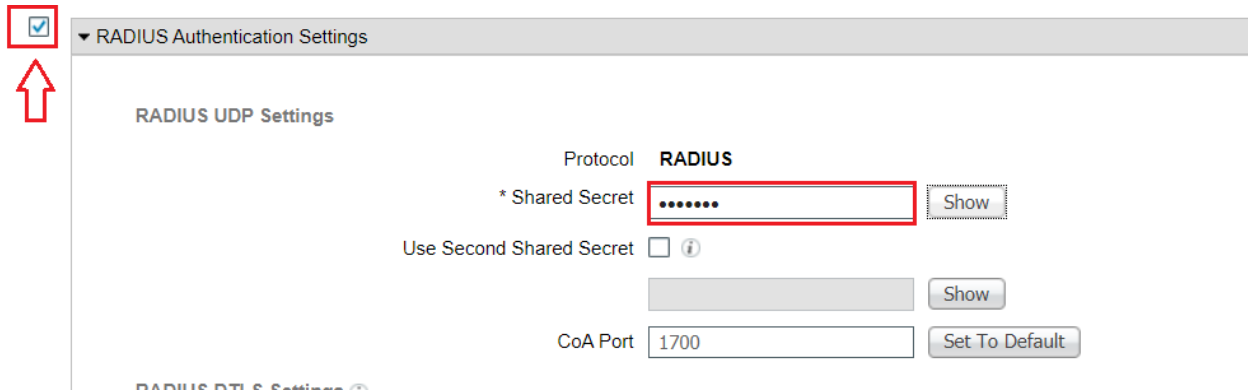
IP Address: * IP: 192.168.100.254 / 32

* Device Profile: Cisco
Model Name: ADVENTERPRI
Software Version: 15.2

* Network Device Group

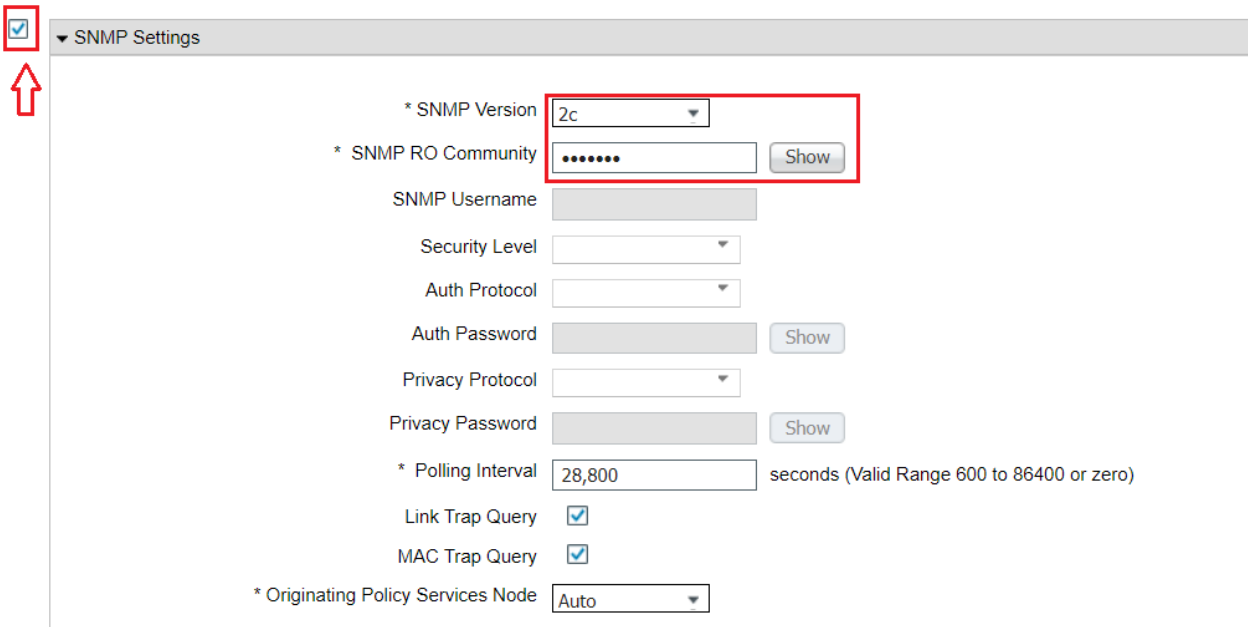
Location: All Locations (Set To Default)
IPSEC: Is IPSEC Device (Set To Default)
Device Type: All Device Types (Set To Default)

Scroll down to set Authentication settings. Set Password configured as Server key on Switch device “Test123” and save settings.

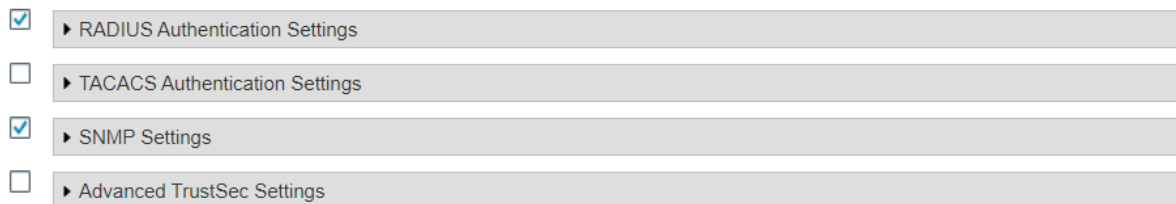


The screenshot shows the 'RADIUS Authentication Settings' page. A red box highlights the 'RADIUS Authentication Settings' header, and a red arrow points to it. Below the header, the 'RADIUS UDP Settings' section is visible. The 'Protocol' is set to 'RADIUS'. The '* Shared Secret' field is highlighted with a red box and contains a masked password '.....'. To its right is a 'Show' button. Below this, the 'Use Second Shared Secret' checkbox is unchecked. Further down, the 'CoA Port' is set to '1700', with a 'Set To Default' button next to it.

Scroll down to check **SNMP Settings** and set **SNMP RO Community** string settings, Click **Submit**.



The screenshot shows the 'SNMP Settings' page. A red box highlights the 'SNMP Settings' header, and a red arrow points to it. The '* SNMP Version' dropdown is set to '2c'. The '* SNMP RO Community' field is highlighted with a red box and contains a masked password '.....', with a 'Show' button to its right. Below this are fields for 'SNMP Username', 'Security Level', 'Auth Protocol', 'Auth Password' (with a 'Show' button), 'Privacy Protocol', and 'Privacy Password' (with a 'Show' button'). The '* Polling Interval' is set to '28,800' seconds. The 'Link Trap Query' and 'MAC Trap Query' checkboxes are both checked. The '* Originating Policy Services Node' dropdown is set to 'Auto'.



The screenshot shows a sidebar with four settings categories, each with a checkbox and a right-pointing arrow: 'RADIUS Authentication Settings' (checked), 'TACACS Authentication Settings' (unchecked), 'SNMP Settings' (checked), and 'Advanced TrustSec Settings' (unchecked).



At the bottom of the settings page, there are two buttons: 'Save' and 'Reset'. The 'Save' button is highlighted with a red box.

Enable Passive ID Service:

First of all, enable the **PassiveID** service. Go to **Administration -> System -> Deployment** and edit the policy server node. Select **Enable Passive Identity Service** and click **Save**.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu at the top includes Home, Context Visibility, Operations, Policy, Administration (highlighted), and Work Centers. Under Administration, the System menu is expanded, showing Deployment (highlighted), Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings.

The main content area displays the **Deployment Nodes List > ise1** and the **Edit Node** configuration for the node 'ise1'. The **General Settings** tab is selected. The configuration shows:

- Hostname: ise1
- FQDN: ise1.test.local
- IP Address: 192.168.100.210
- Node Type: Identity Services Engine (ISE)

The Role is set to **PRIMARY**, and there is a **Make Standalone** button. The following services are checked:

- Administration
- Monitoring
- Policy Service
 - Enable Session Services (checked)
 - Include Node in Node Group: None
 - Enable Profiling Service (checked)
 - Enable Threat Centric NAC Service (unchecked)
 - Enable SXP Service (unchecked)
 - Enable Device Admin Service (checked)
 - Enable Passive Identity Service (checked)** (highlighted with a red box and an arrow)

show application status ise | i PassiveID

The screenshot shows a PuTTY terminal window titled '192.168.100.210 - PuTTY'. The output of the command 'show application status ise | i PassiveID' is displayed:

```
Failed to log in 1 time(s)
Last failed login on Wed Jul 14 13:34:11 2021 from tty1
ise1/admin#
ise1/admin# sh application status ise | i PassiveID
PassiveID WMI Service          running          24225
PassiveID Syslog Service       running          24878
PassiveID API Service          running          25678
PassiveID Agent Service        running          26611
PassiveID Endpoint Service     running          27186
PassiveID SPAN Service         running          27710
```

Passive ID Configuration:

Select **PassiveID** menu on the right and click on “**Add DCs**”.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Work Centers' dropdown is open, showing 'PassiveID'. The 'PassiveID' menu is highlighted. The left sidebar shows 'Providers' with 'Active Directory' selected. The main content area shows 'PassiveID Domain Controllers' with a table of domain controllers. The 'Add DCs' button is highlighted in the table.

Domain	DC Host	Site
test.local	srv.test.local	Default-First-Site-Name

A popup appears; select your **DC host** and click **OK**.

Add Domain Controllers

1 Selected

Domain	DC Host	Site
test.local	srv.test.local	Default-First-Site-Name

Cancel

OK

Select the domain just inserted and click **Edit**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Work Centers' dropdown is open, showing 'PassiveID'. The 'PassiveID' menu is highlighted. The left sidebar shows 'Providers' with 'Active Directory' selected. The main content area shows 'PassiveID Domain Controllers' with a table of domain controllers. The 'test.local' domain is selected, and the 'Edit' button is highlighted.

Domain	DC Host	Site	IP Address	Monitor Using
test.local	srv.test.local	Default-First-Site-Name	192.168.100.230	WMI

A popup appears; compile the fields **Username/Password** and press **Save**.

Edit Item



Edit Domain Controller

Host FQDN

Description

User Name *

Password

Protocol

Select the domain and click on the **Config WMI** button to initiate the WMI connection.

Connection Whitelisted Domains **PassiveID** Groups Attributes Advanced Settings

PassiveID Domain Controllers

1 Selected

<input checked="" type="checkbox"/>	Domain	DC Host	Site	IP Address
<input checked="" type="checkbox"/>	test.local	srv.test.local		168.100.230

Config WMI in process...
Configuration of WMI has begun and will take some time.
Status will be shown on completion.Run in background?

After few seconds, a popup gives back the result: Once registration goes fine, ISE will begin monitoring AD for Windows logon events.

Successfully configured 1/1 DC

Configure Downloadable ACL:

Navigate to **Policy > Policy Elements > Results > Authorization > Downloadable ACLs** click **Add**

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', and 'Administration'. The 'Policy' menu is expanded, showing 'Policy Sets', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. The 'Policy Elements' menu is further expanded, showing 'Dictionary', 'Conditions', and 'Results'. The 'Results' menu is expanded, showing 'Authentication', 'Authorization', 'Profiling', and 'Posture'. The 'Authorization' menu is expanded, showing 'Authorization Profiles' and 'Downloadable ACLs'. The 'Downloadable ACLs' page is displayed, showing a table of existing ACLs. A red box highlights the 'Add' button in the top right corner of the table.

Name	Description
ACL_Test	
DENY_ALL_IPV4_TRAFFIC	Deny all ipv4 traffic
DENY_ALL_IPV6_TRAFFIC	Deny all ipv6 traffic
PERMIT_ALL_IPV4_TRAFFIC	Allow all ipv4 Traffic
PERMIT_ALL_IPV6_TRAFFIC	Allow all ipv6 Traffic

Create a DACL with Name **DACL_Easyconnect**. Permit DNS, DHCP and AD Services and deny rest of all traffic Click **Save**.

The screenshot shows the 'Downloadable ACL List > DACL_Easyconnect' page. The 'Downloadable ACL' form is displayed. The 'Name' field is set to 'DACL_Easyconnect'. The 'Description' field is empty. The 'IP version' is set to 'IPv4'. The 'DACL Content' field contains the following text:

```
1234567 permit udp any any eq 53
8910111 permit udp any eq 68 any eq 67
2131415 permit ip any host 192.168.100.230
1617181 deny ip any any
9202122
2324252
6272829
3031323
3343536
3738394
```

A red arrow points to the 'Save' button at the bottom left of the form. The 'Check DACL Syntax' button is also visible.

Create DACL for Employees with Name **DACL_Employees**. Permit all IP traffic Click **Save**.

Downloadable ACL List > **DACL_Employees**

Downloadable ACL

* Name **DACL_Employees**

Description

IP version ☒ IPv4 ☐ IPv6 ☐ Agnostic ⓘ

* DACL Content

1234567	permit ip any any
8910111	
2131415	
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	

Check DACL Syntax

Save Reset

Create DACL for Contractor with Name **DACL_Contractor**. Deny ICMP and TCP traffic and Permit all other IP traffic Click **Save**.

Downloadable ACL List > **DACL_Contractor**

Downloadable ACL

* Name **DACL_Contractor**

Description

IP version ☒ IPv4 ☐ IPv6 ☐ Agnostic ⓘ

* DACL Content

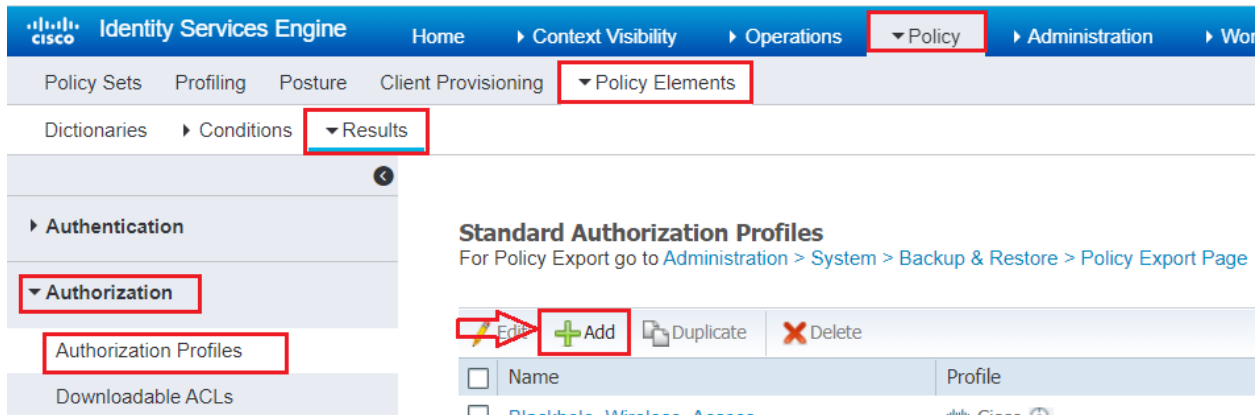
1234567	deny icmp any host 192.168.100.12
8910111	deny tcp any host 192.168.100.12
2131415	permit ip any any
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	

Check DACL Syntax

Save Reset

Configure Authorization Profiles:

Now add this DACL to a new Authorization Profile. **Policy > Policy Elements > Results > Authorization > Authorization Profiles** Click **Add**

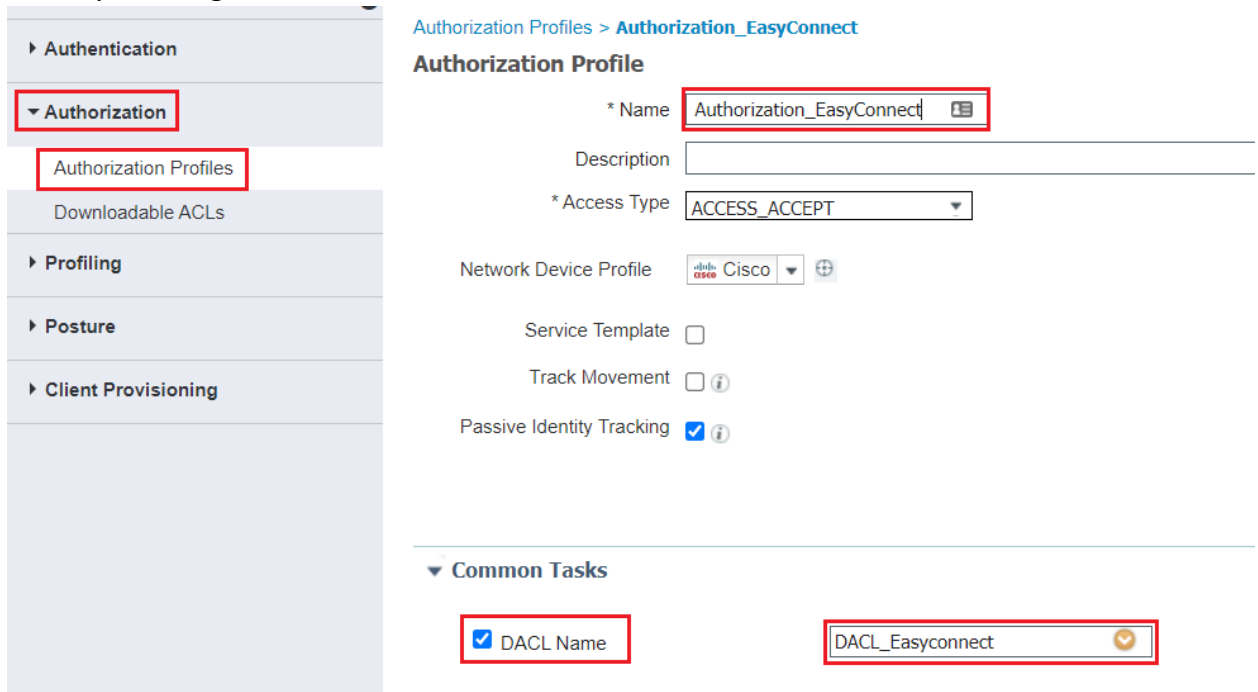


Standard Authorization Profiles
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

[Add](#) [Duplicate](#) [Delete](#)

Name	Profile
Blackhole_Wireless_Access	adobe Cisco

Name Authorization profile in this case **Authorization_EasyConnect**. Select DACL Name from the drop-down list select the DACL previously configured called **DACL_Easyconnect**. Tick Passive Identity Tracking and Click **Save**.



Authorization Profile

* Name:

Description:

* Access Type:

Network Device Profile:

Service Template: ☐

Track Movement: ☐

Passive Identity Tracking: ☒

Common Tasks

☒ DACL Name:

Name Authorization profile in this case **Authorization_Employees**. Select DACL Name from the drop-down list select the DACL previously configured called **DACL_Employees** and Click **Save**.

Authorization Profiles > **Authorization_Employees**

Authorization Profile

* Name **Authorization_Employees**

Description

* Access Type **ACCESS_ACCEPT**

Network Device Profile **Cisco**

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

▼ **Common Tasks**

☒ DACL Name **DACL_Employees**

Name Authorization profile in this case **Authorization_Contractor**. Select DACL Name from the drop-down list select the DACL previously configured called **DACL_Contractor** and Click **Save**.

Authorization Profiles > **Authorization_Contractor**

Authorization Profile

* Name **Authorization_Contractor**

Description

* Access Type **ACCESS_ACCEPT**

Network Device Profile **Cisco**

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

▼ **Common Tasks**






☒ DACL Name **DACL_Contractor**

Policy Set:












A policy set is a hierarchical container consisting of a single user-defined rule that indicates the allowed protocol or server sequence for network access, as well as authentication and authorization policies and policy exceptions, all also configured with user-defined condition-based rules.

In order to create a Policy Set from ISE GUI, navigate to **Policy > Policy Set** and then click on plus (+) icon on the upper-left corner.

Policy Sets

	Status	Policy Set Name	Description	Conditions
				
		Dot1x-Policy Set	Dot1 x Policy for Wired	 Wired_802.1X
		Default	Default policy set	



Name the Policy Set in this case **EassyConnect-Policy**, set the Conditions **Wired_MAB** and Set the **Allow Protocols** Default Network Access protocols. Click **Save** to apply the setting.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
	EassyConnect-Policy	EassyConnect-Policy	 Wired_MAB	Default Network Access x 
	EAP-TLS-Policy	EAP-TLS-Policy	 DEVICE: Device Type EQUALS All Device Types	Allowed-EAP-TLS x 
	Dot1x-Policy Set	Dot1 x Policy for Wired	 Wired_802.1X	Default Network Access x 
	Default	Default policy set		Default Network Access x 

Authentication Policy:






For network access policies, choose **Work Centers > Network Access > Policy Sets**. Navigate to Authentication Policy, click Add new **authentication policy**.

▼ Authentication Policy (1)



	Status	Rule Name	Conditions
			

Name Authentication Policy Rule in this case **Auth-Easyconnect** set the conditions to **Wired_MAB** also change the default Identity store to **AD_Internal_Store** which we created earlier. Change the Default Rule Options to **DenyAccess**.

▼ Authentication Policy (2)

	Status	Rule Name	Conditions	Use
				
		Auth-Easyconnect	 Wired_MAB	AD_Internal_Store x ▼ ➤ Options
		Default		DenyAccess x ▼ ➤ Options

Leave the default **Options** settings and click **Save** to apply the changes.

	Auth-Easyconnect	 Wired_MAB	AD_Internal_Store x ▼ ▼ Options If Auth fail REJECT x ▼ If User not found REJECT x ▼ If Process fail DROP x ▼
---	------------------	---	--

Authorization Polices:

Navigate to **Policy>Policy Sets > click on Arrow Icon >**

Policy Sets

Reset Policyset Hitcounts								
Reset								
Save								
+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Search								
	✓	EAP-TLS Policy		Wired_802.1X	EAP-TLS and MAB	0	⚙️ ➡️ ➤	
	✓	Dot1x-Policy Set	Dot1 x Policy for Wired	Wired_802.1X	Default Network Access	0	⚙️ ➤	
	✓	Default	Default policy set		Default Network Access	0	⚙️ ➤	

Navigate to **Authorization Policy** section click on **round circle Plus** icon to add new Authorization rules, name authorization Rules in this case **Employees, Contractor and EasyConnect**. In **Conditions** click on **Plus** icon to set the conditions for authorization Rules.

Authorization Policy (14)			
+	Status	Rule Name	Conditions
Search			

In **Employees** **AD-Test.Local-ExternalGroups EQUALS test.local/users/Employees, Authorization_Employees**

In **Contractor** **AD-Test.Local-ExternalGroups EQUALS test.local/users/Contractor, Authorization_Contactor**

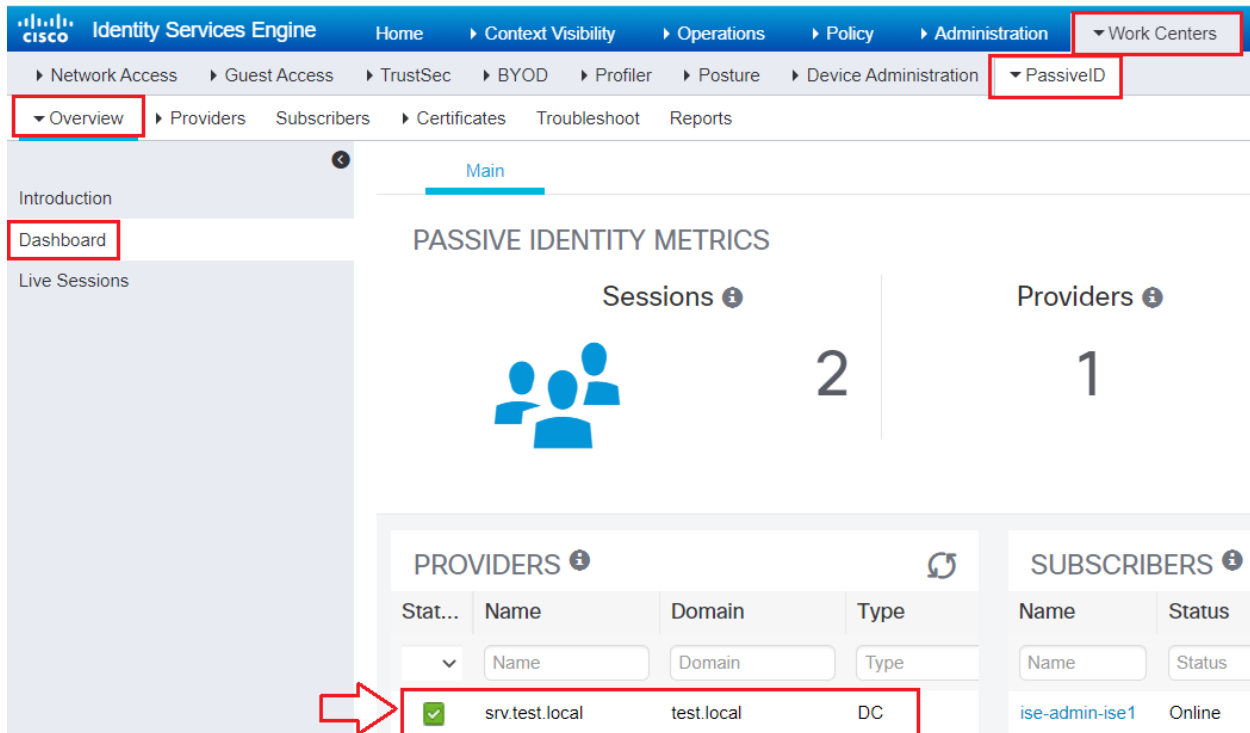
In **EasyConnect** **Wired_MAB Authorization_EasyConnect**

+	Status	Rule Name	Conditions	Results
				Profiles
Search				
	✓	Employees	AD-Test.Local-ExternalGroups EQUALS test.local/ISE-Groups/Employees	× Authorization_Employees +
	✓	Contractor	AD-Test.Local-ExternalGroups EQUALS test.local/ISE-Groups/Contractor	× Authorization_Contractor +
	✓	EasyConnect	Wired_MAB	× Authorization_EasyConnect +
	✓	Default		× DenyAccess +

Reset Save

Verification:

To view a brief summary of the PassiveID info, click on the **Dashboard** link.



PROVIDERS

Stat...	Name	Domain	Type
<input checked="" type="checkbox"/>	srv.test.local	test.local	DC

SUBSCRIBERS

Name	Status
ise-admin-ise1	Online

To view any session learned via PassiveID, click on the **“Live Sessions”** link.

Refresh Export To

Session Status	Action	Endpoint ID	Identity	IP Address	Endpoint Profile
<input type="text"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Authenticated	Show Actions	50:01:00:0A:00:00	c1	192.168.20.12	FreeBSD-Workstation
Authenticated	Show Actions	192.168.100.210	Administrator	192.168.100.210	

Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	50:01:00:0A:00:00				
c1	50:01:00:0A:00:00	FreeBSD-W...			
50:01:00:0A:00:00	50:01:00:0A:00:00	FreeBSD-W...	EasyConne...	EasyConne...	Authorizatio...
	50:01:00:0A:00:00				
#ACSACL#-IP-DA...					