

Configure Change of Authorization in Catalyst 1300 Using Web User Interface

Objective

The objective of this article is to show you how to configure change of authorization (CoA) in Catalyst 1300 switches using the web user interface (UI).

Applicable Devices and Software Version

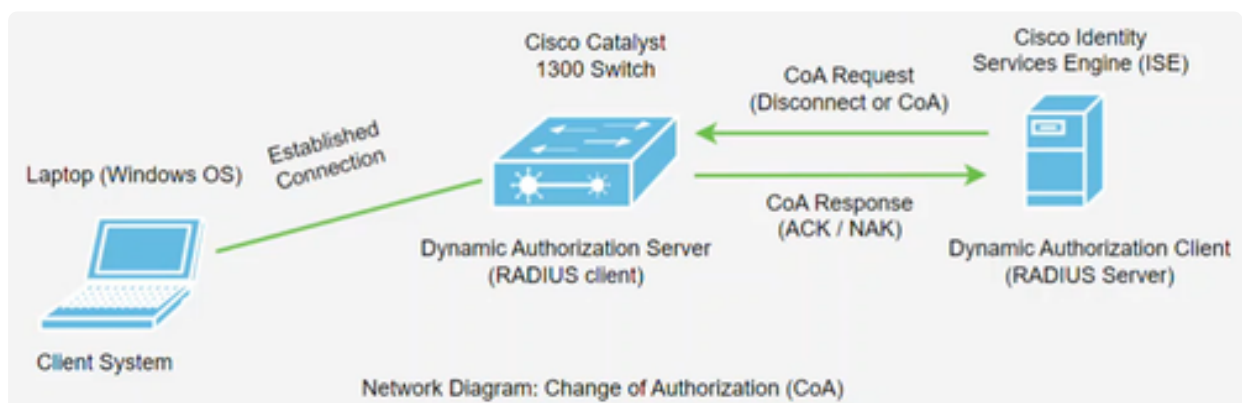
- Catalyst 1300 switches | 4.1.6.53

Introduction

Change of Authorization (CoA) is an extension to the RADIUS protocol, that allows you to change the properties of an authentication, authorization, and accounting (AAA) or dot1x user session after it has been authenticated. When a policy for a user or group in AAA changes, administrators can transmit RADIUS CoA packets from the AAA server, such as a Cisco Identity Services Engine (ISE), to reinitialize authentication and apply the new policy.

The Cisco Identity Services Engine (or ISE) is a fully featured Network Based Access Control and Policy Enforcement Engine. It provides security analysis and enforcement, RADIUS and TACACS services, policy distribution, and more. Cisco ISE is currently the only supported CoA Dynamic Authorization Client for Catalyst 1300 switches. Refer to the [ISE Admin guide](#) for more information.

This feature requires communication between the Dynamic Authorization Client (RADIUS Server) and the Dynamic Authorization Server (Catalyst switch). As seen in network diagram below, the Dynamic Authorization Server sends a disconnect or CoA message to the Dynamic Authorization Server and the switch provides a response.



The CoA support has been added to the Catalyst 1300 switches in firmware version 4.1.3.36. This includes support for disconnecting users and changing authorizations applicable to a user session. The device supports the following CoA actions:

- Disconnect Session
- Disable host port CoA command
- Bounce host port CoA command
- Reauthenticate host CoA command

To configure CoA using command line interface (CLI), refer to [Configuration of Change of Authorization in Catalyst 1300 Switch using CLI](#).

Table of Contents

- [Configuring Catalyst 1300 RADIUS Client on ISE](#)
- [Configurations in Catalyst 1300 Switch](#)
- [CoA Operation](#)

Configuring Catalyst 1300 RADIUS Client on ISE

In this example, Cisco ISE server version 3.2 is used. For an overview of ISE, check out the [Cisco Identity Services Engine](#) product page.

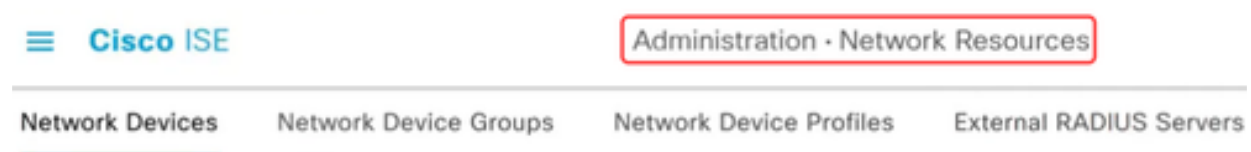
Note:

CoA is supported on ISE version 2.7 and later.

After deploying Cisco ISE server, log in to access the web UI.

Step 1

To add network devices, navigate to the **Administration > Network Resources** menu.



Step 2

Click on the + **Add** button.

Network Devices



Step 3

Enter the *Name*, *Description*, and *IP address* of the Catalyst switch.

Network Devices

Name	C1300-24FP
Description	Catalyst 1300 switch
IP Address	* IP : 172.19.1.250 / 32

Step 4

From the *Device Profile* drop-down menu, select **Cisco**.

Step 5

Configure the *RADIUS Authentication Settings* by entering the *Shared Secret*.



▼ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

RADIUS

Shared Secret

●●●●●●●●

[Show](#)

Step 6

Enter the *CoA Port* number. The default port is **1700**.

CoA Port

1700

[Set To Default](#)

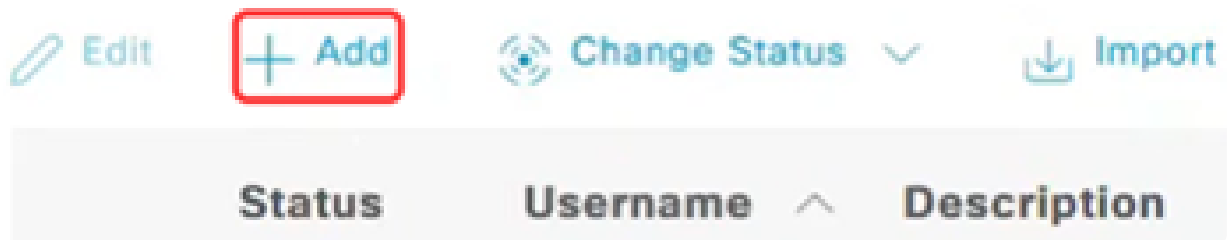
Step 7

Next, navigate to **Administration > Identity Management** and select **Network Access Users**.

Step 8

To define the username and password, click on the **+Add** symbol.

Network Access Users



Step 9

Enter the username, password and click **Save** at the bottom of the page.

Network Access User

* Username

test1

Status



Enabled



Configurations in Catalyst 1300 Switch

Step 1

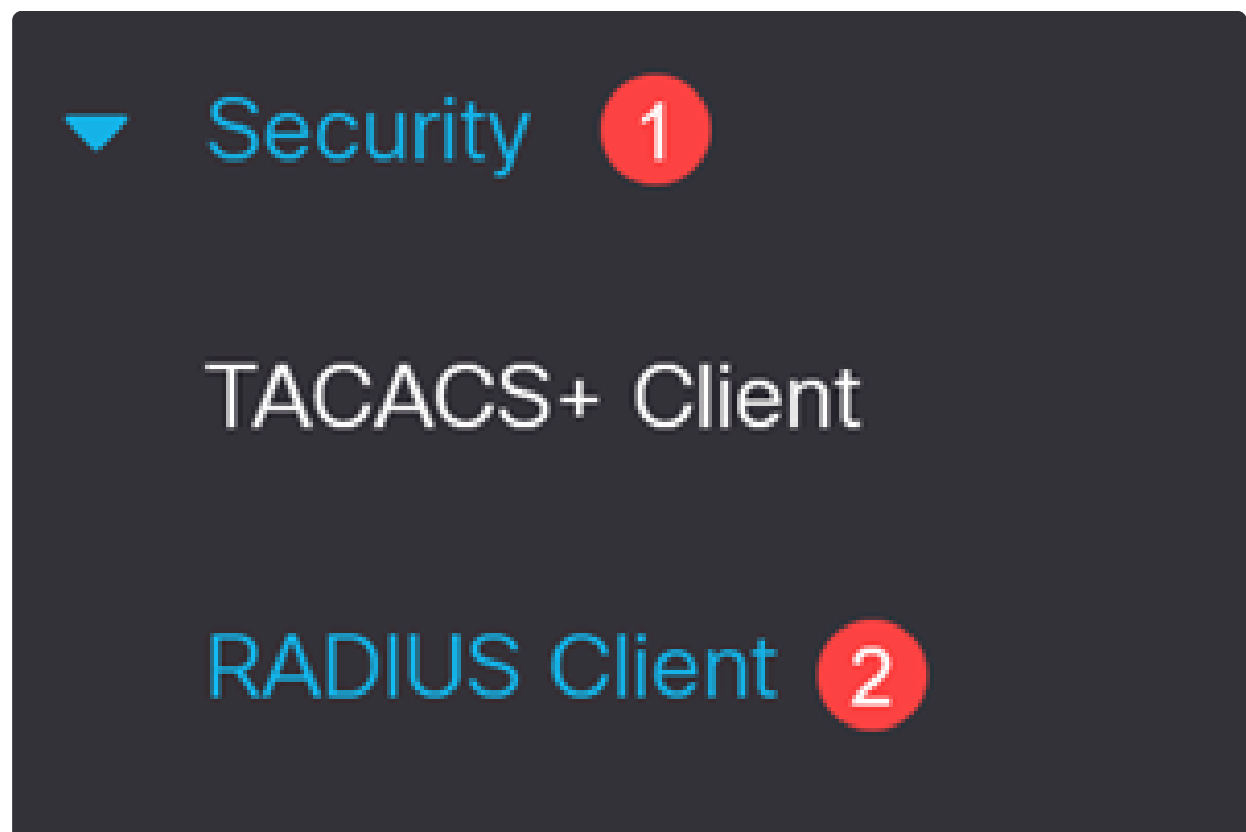
Login to your Catalyst 1300 switch and select **Advanced** mode. In this example, C1300-24FP-4X is used.

Note:

The CoA support has been added to the Catalyst 1300 switches in firmware version 4.1.3.36.

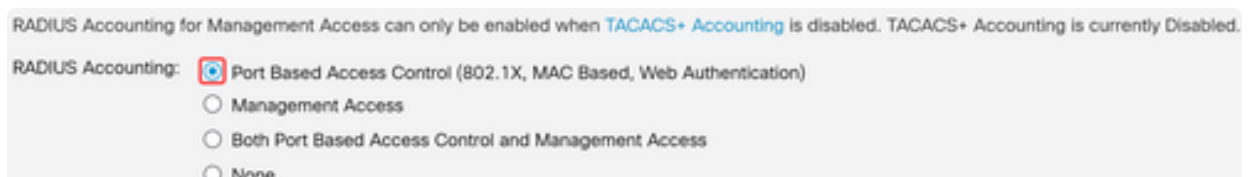
Step 2

Navigate to the **Security > RADIUS Client** in the navigation pane.



Step 3

Set *RADIUS Accounting* to **Port Based Access Control**.



Step 4

To add the ISE server, scroll down to the *RADIUS Table* and click on the **plus icon**.

Step 5

Configure the RADIUS server settings.

- Select *Server Definition*. In this example, **By IP address** is selected. Enter the IP address in the *Server IP Address/Name* field.
- Set a *RADIUS Priority*.
- Authentication and Accounting Ports are set to the default.
- *Usage Type* is 802.1x.

Click **Apply**.

Add RADIUS Server

Server Definition:	<input checked="" type="radio"/> By IP address <input type="radio"/> By name
IP Version:	<input type="radio"/> Version 6 <input checked="" type="radio"/> Version 4
IPv6 Address Type:	<input checked="" type="radio"/> Link Local <input type="radio"/> Global
Link Local Interface:	VLAN 1
Server IP Address/Name:	192.168.251.100 1
Priority:	1 (Range: 0 - 65535) 2
Key String:	<input checked="" type="radio"/> Use Default <input type="radio"/> User Defined (Encrypted) <input type="text"/> <input type="radio"/> User Defined (Plaintext) <input type="text"/> (0/128 characters used)
Timeout for Reply:	<input checked="" type="radio"/> Use Default <input type="radio"/> User Defined Default <input type="text"/> sec (Range: 1 - 30, Default: 3)
Authentication Port:	1812 (Range: 0 - 65535, Default: 1812) 3
Accounting Port:	1813 (Range: 0 - 65535, Default: 1813)

Step 6

To configure 802.1x authentication, navigate to **Security > 802.1X Authentication > Properties** menu.

▼ 802.1X Authentication

Properties

Step 7

Ensure that *Port-Based Authentication* is enabled, and *Authentication Method* is set to **RADIUS**.

Properties

Port-Based Authentication:

☒ Enable

Authentication Method:

☐ RADIUS, None

☒ RADIUS

☐ None

Step 8

Navigate to **Port Authentication** menu, select the desired port, and click **edit**.

▼ 802.1X Authentication

Properties

Port Authentication

Step 9

For *Administrative Port Control*, select **Auto** option that will switch the port between authorized and unauthorized state based on the RADIUS response.

Edit Port Authentication

Interface:

Unit

1 ▼

Port

GE4 ▼

Current Port Control:

Authorized

Administrative Port Control:

☐ Force Unauthorized

☒ Auto

☐ Force Authorized

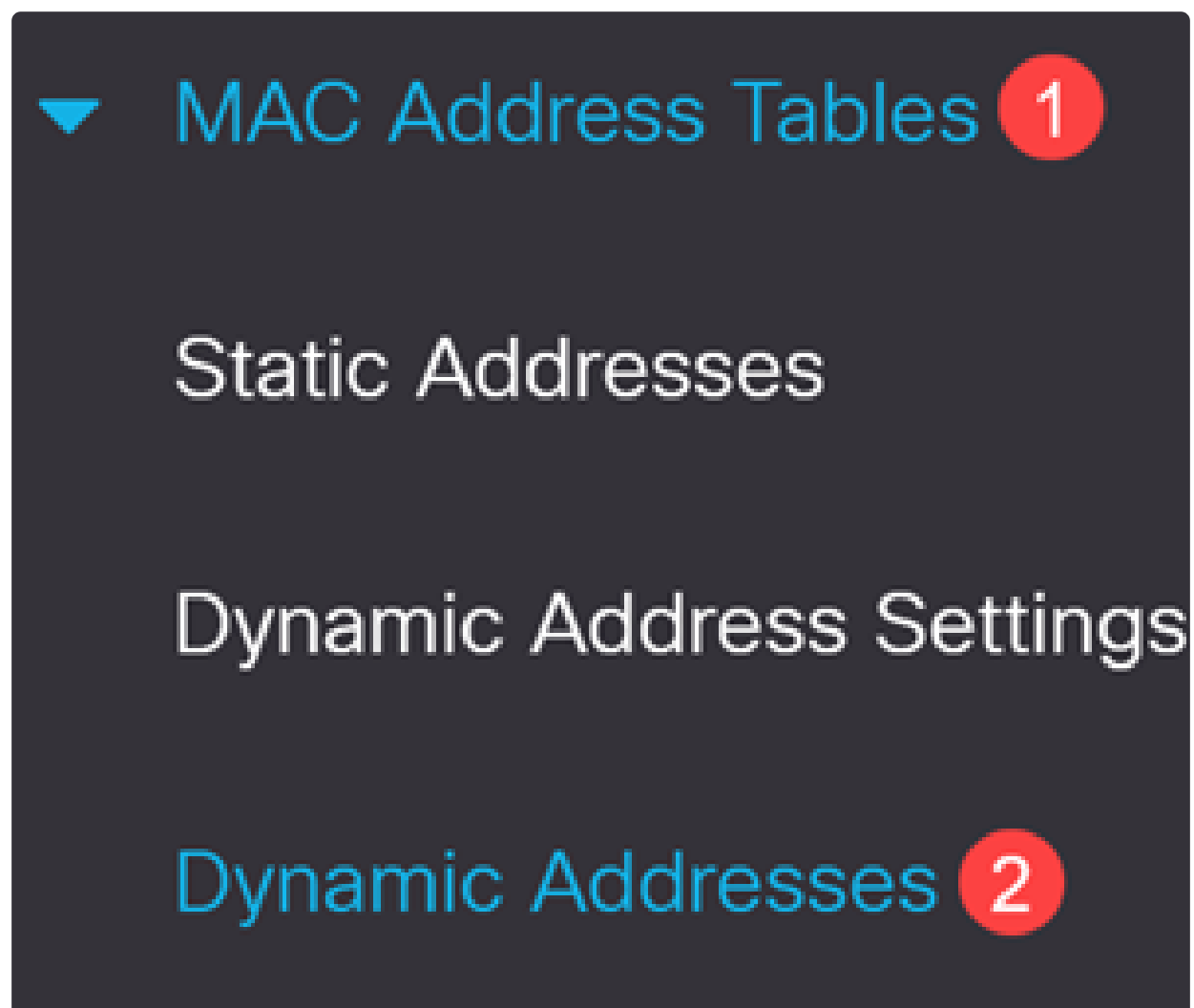
Step 10

Enable *802.1x Based Authentication* and click **Apply**.

802.1x Based Authentication: ☒ Enable

Step 11

You will need the MAC address for the device on the port. The CoA operation on ISE will be applied to that MAC address. In this example, it is port 9. To get it, navigate to **MAC Address Tables > Dynamic Addresses**.

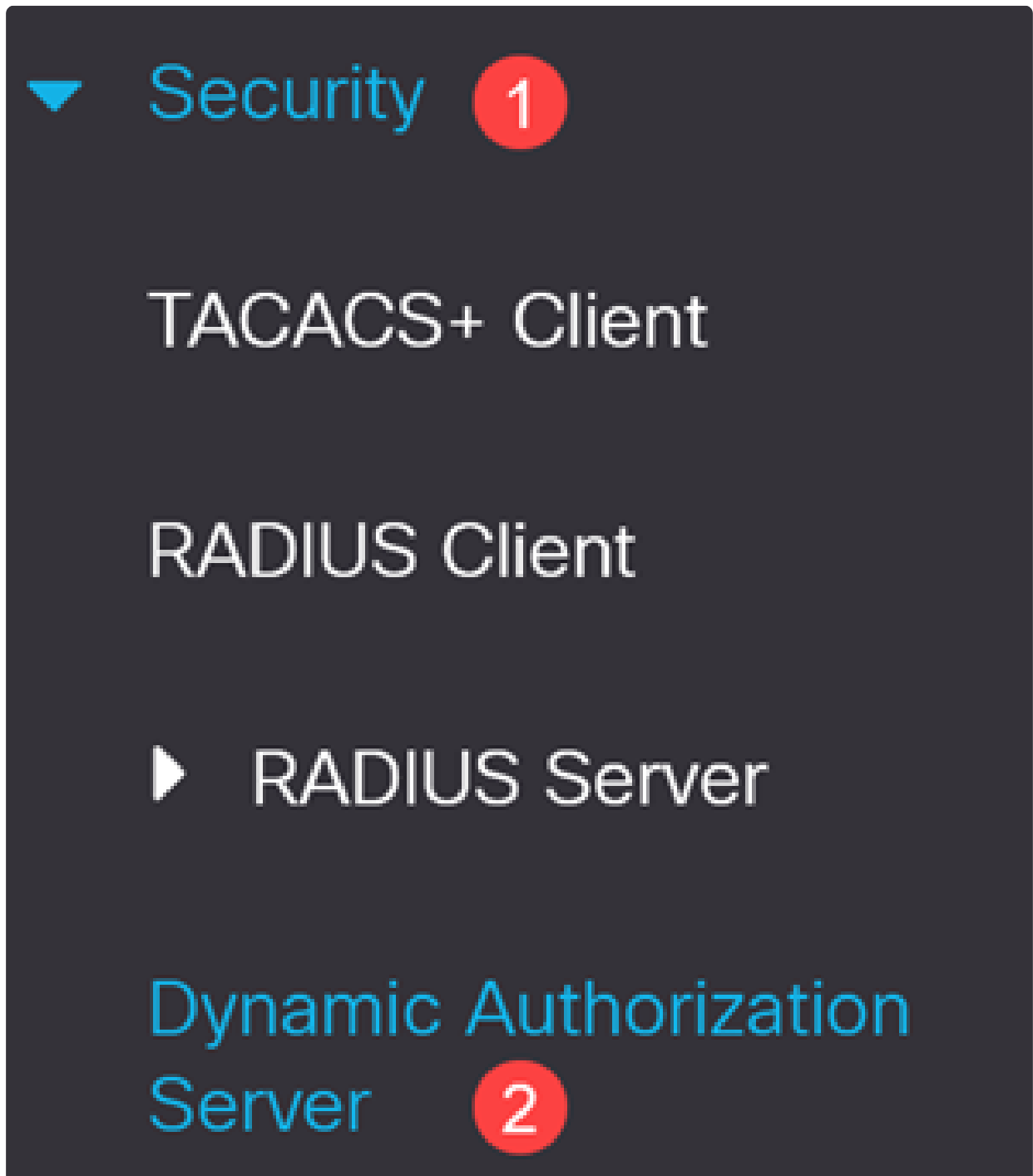


Step 12

Scroll down to the port and note the MAC address.

Step 13

Navigate to **Security > Dynamic Authorization Server**.



Step 14

Enable the following:

- Enforce Server Key Match

- Enforce Timestamp on Rx
- Handle Disable Port Commands
- Handle Bounce Port Commands

Dynamic Authorization Server

Enforce Server Key Match: ☒ Enable

Enforce Timestamp on Rx: ☒ Enable

Handle Disable Port Commands: ☒ Enable

Handle Bounce Port Commands: ☒ Enable

Step 15

Leave the *UDP Port* at the default value of **1700**.

UDP Port: (Range: 0 - 59999, Default: 1700)

Step 16

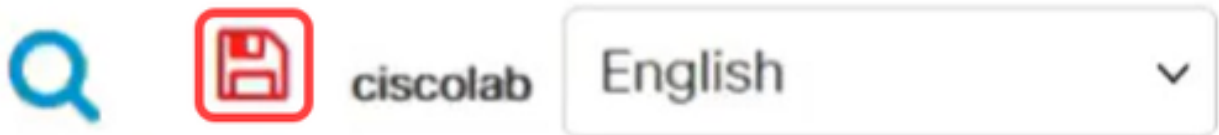
Under *Client Table*, make sure the ISE server is added with the correct server key. Click **Apply**.

+

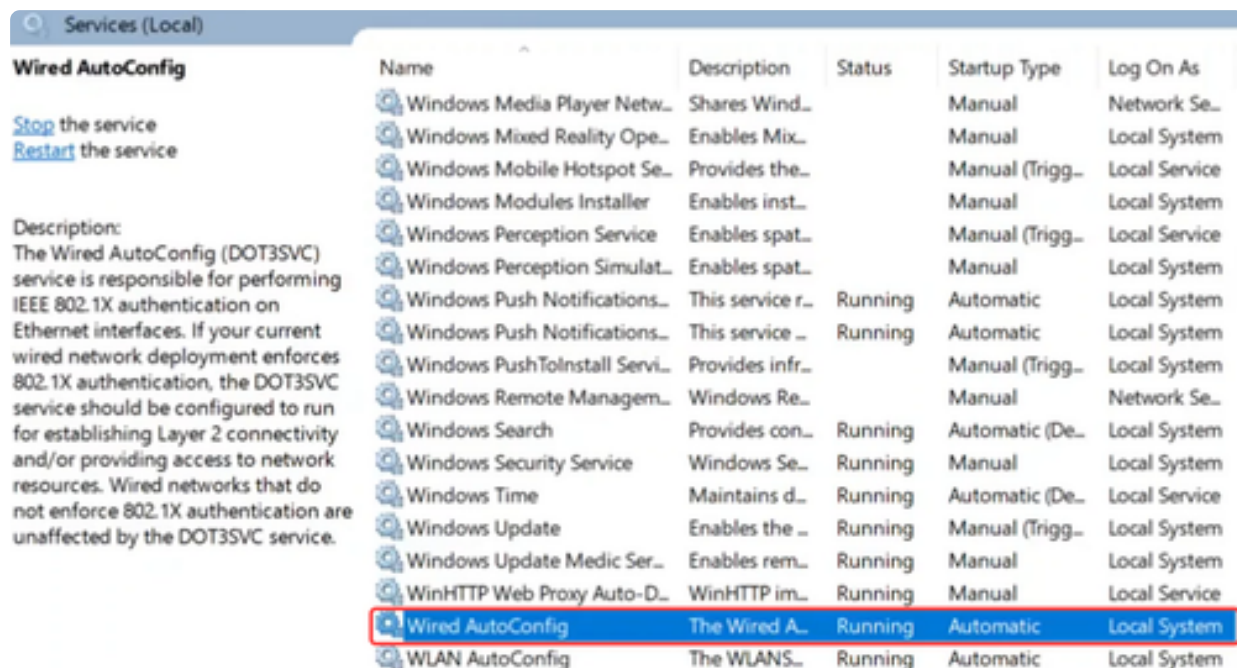
Counters

<input type="checkbox"/>	Client Address	Server Key MD5
<input type="checkbox"/>	192.168.1.115	12d...ba6

Click the red blinking **Save** icon to save the configurations.

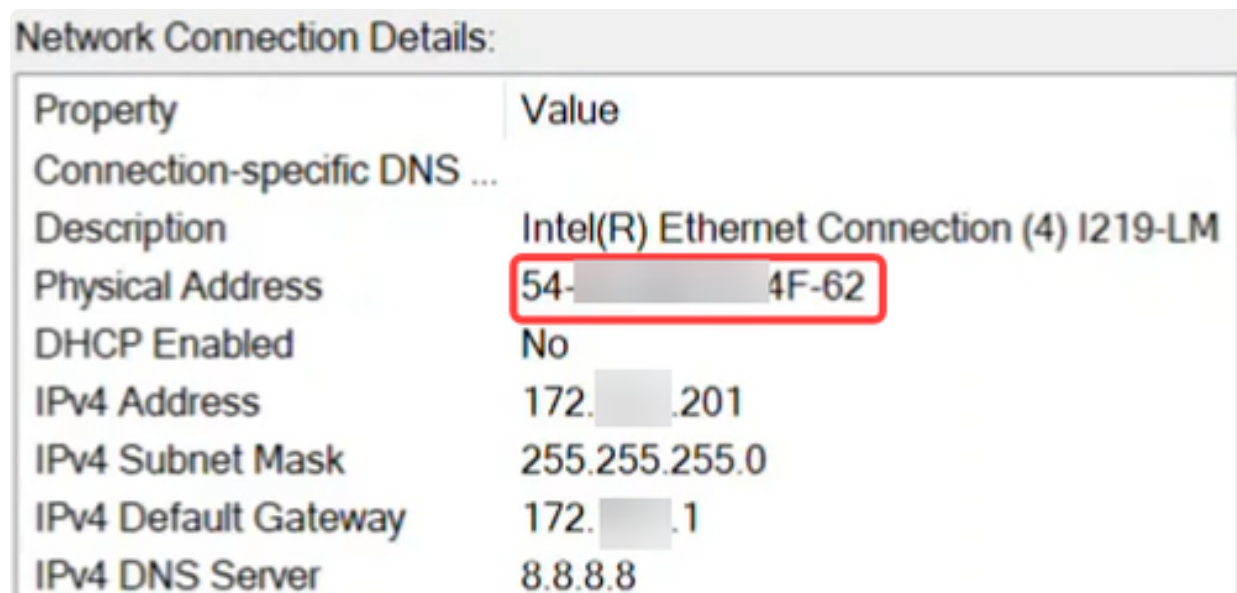


On the client laptop connected to port 9, verify the **Wired AutoConfig** service is enabled for 802.1 X authentication.



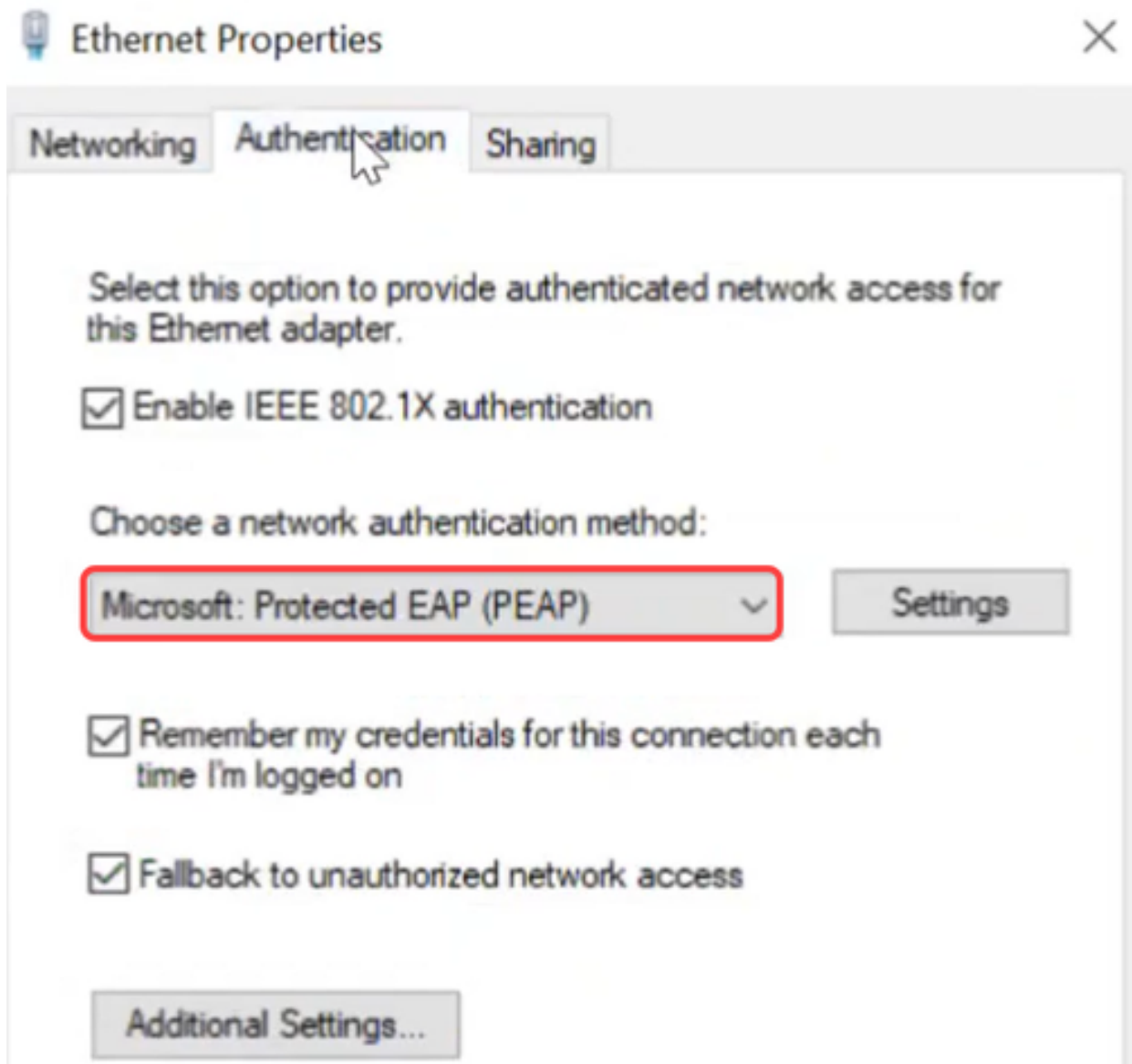
Step 19

On the *Ethernet* adapter settings, verify that the MAC address matches.



Step 20

Click the **Properties** button under Ethernet settings and under the **Authentication** tab, make sure the check boxes are enabled. Also, make sure the authentication method is **Protected EAP (PEAP)**.



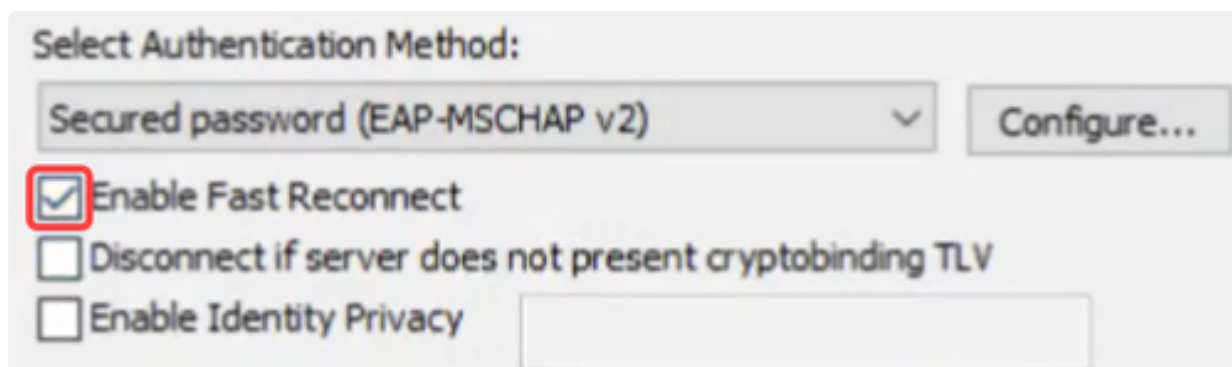
Step 21

Click the **Settings** button to make sure the check box next to *Verify the server's identity by validating the certificate* is unchecked.



Step 22

Enable Fast Reconnect box should be checked.



Select Authentication Method:

Secured password (EAP-MSCHAP v2) Configure...

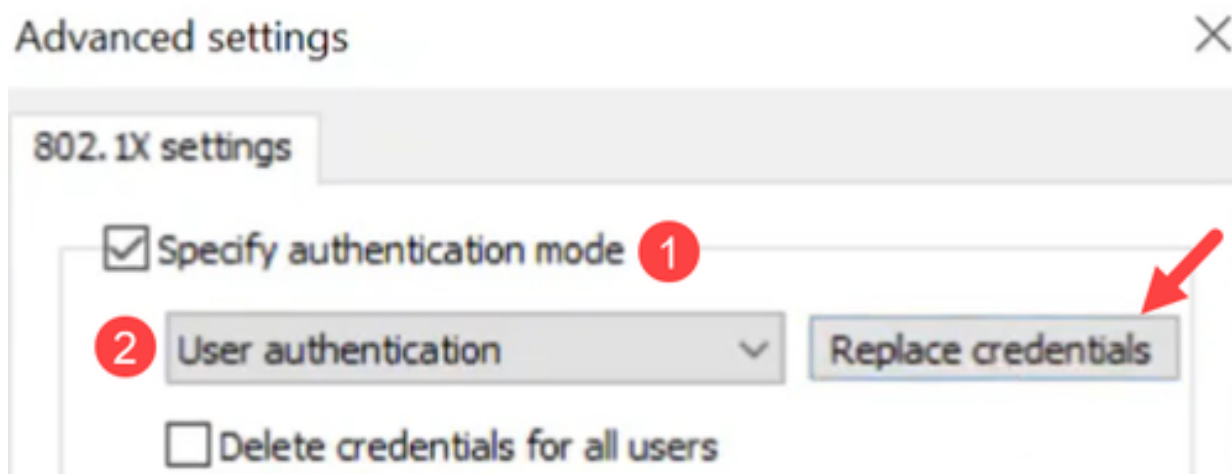
☒ Enable Fast Reconnect

☐ Disconnect if server does not present cryptobinding TLV

☐ Enable Identity Privacy

Step 23

Under Additional settings, make sure **Specify authentication mode** is enabled, and **User authentication** is selected from the drop-down menu. You can save the credentials created on ISE or replace it using *Replace credentials* button.



Advanced settings ×

802.1X settings

☒ Specify authentication mode 1

2 User authentication ▼ Replace credentials

☐ Delete credentials for all users

CoA Operation

Before initiating CoA operation, enable packet capture on the switch.

Step 1

On PuTTY, login to your Catalyst switch and specify the buffer size and capture mode by using the command *monitor capture cap1 buffer size 20 circular*.

Step 2

Specify the control plane as both by using the command *monitor capture cap1 control-plane both*.

Step 3

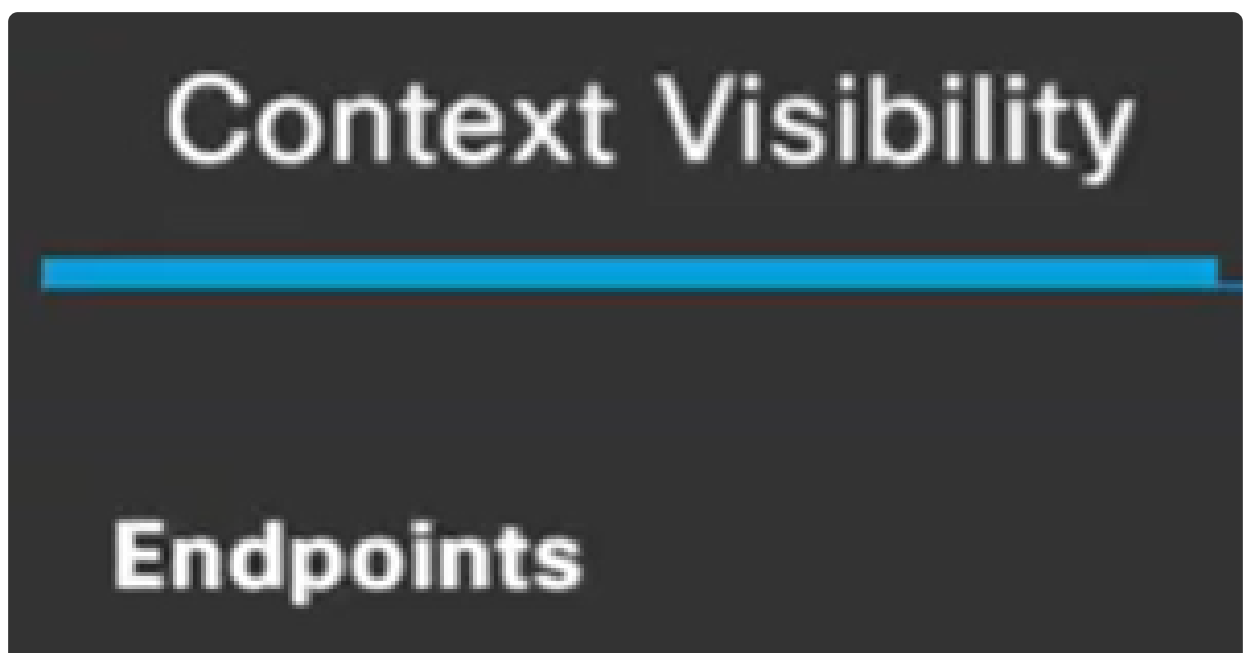
Enter the match criteria as any. The command for this will be *monitor capture cap1 match any*.

Step 4

Start the packet capture.

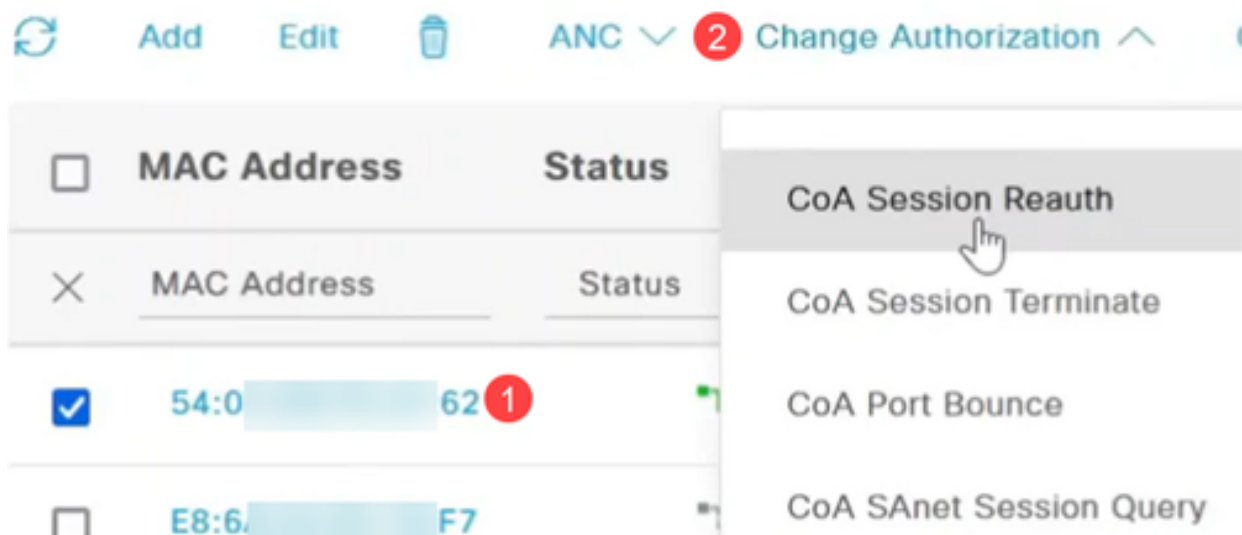
Step 5

On ISE interface, navigate to **Endpoints** option under **Context Visibility**.



Step 6

Choose the **MAC address** and select the CoA operation from the *Change of Authorization* drop-down menu. In this example, **CoA Session Reauth** is selected. This forces re-authentication on the port by sending a CoA packet with a reauthenticate command.



Step 7

Go back to the PuTTY terminal to check if the CoA operation was successful.

```
Started capture point : cap1
Cat1300-1#04-Jul-2024 20:49:45 %SEC-W-COAREAUTHSESSN: 802.1x re-authentication initiated for host 54:00:00:00:00:00:62 by CoA Request "reauthenticate"
```

Step 8

If you select *CoA Session Terminate*, it will send a disconnect request with a terminate command based on an administrative request.

```
Cat1300-1#04-Jul-2024 20:50:02 %SEC-W-PORTUNAUTHORIZED: Port gil/0/9 is unauthorized
04-Jul-2024 20:50:02 %SEC-W-COAPDISCSESSN: 802.1x session for host 54:00:00:00:00:00:62 on interface gi1/0/9 has been terminated by Disconnect-Request. Authenticator state on the Interface will be re-initialized
04-Jul-2024 20:50:02 %SEC-I-PORTAUTHORIZED: Port gil/0/9 is Authorized
```

Step 9

CoA Port Bounce option will send a CoA request packet with a bounce host port command, disabling and re-enabling the port on the switch. The network adapter goes offline for 10 seconds and becomes unauthorized. It will come back online, becomes authorized and can forward packets.

```

Cat1300-1#04-Jul-2024 20:50:21 %SEC-W-COABNCEPORT: Interface gil/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54: :62
04-Jul-2024 20:50:21 %LINK-W-Down: gil/0/9
04-Jul-2024 20:50:34 %LINK-I-Up: gil/0/9
04-Jul-2024 20:50:34 %SEC-W-PORTUNAUTHORIZED: Port gil/0/9 is unAuthorized
04-Jul-2024 20:50:36 %LINK-W-Down: gil/0/9
04-Jul-2024 20:50:39 %LINK-I-Up: gil/0/9
04-Jul-2024 20:50:39 %SEC-I-PORTAUTHORIZED: Port gil/0/9 is Authorized
Cat1300-1#04-Jul-2024 20:50:45 %STP-W-PORTSTATUS: gil/0/9: STP status Forwarding

```

Step 10

CoA Session termination with port bounce will terminate the existing session, bounce the port for 10 seconds, and become unauthorized. It then comes back online, becomes authorized and can forward packets.

```

Cat1300-1#04-Jul-2024 20:51:04 %SEC-W-COABNCEPORT: Interface gil/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54: :62
04-Jul-2024 20:51:04 %LINK-W-Down: gil/0/9
04-Jul-2024 20:51:22 %LINK-I-Up: gil/0/9
04-Jul-2024 20:51:22 %SEC-W-PORTUNAUTHORIZED: Port gil/0/9 is unAuthorized
04-Jul-2024 20:51:22 %SEC-I-PORTAUTHORIZED: Port gil/0/9 is Authorized
04-Jul-2024 20:51:29 %STP-W-PORTSTATUS: gil/0/9: STP status Forwarding

```

Step 11

CoA session termination with port shutdown will terminate the session and administratively shut down the port.

```

Cat1300-1#04-Jul-2024 20:51:47 %SEC-W-COADISPORT: Interface gil/0/9 suspended by CoA Request "disab
le host port" for host 54: :62
04-Jul-2024 20:51:47 %LINK-W-Down: gil/0/9

```

Step 12

To stop the packet capture, use the command **monitor capture cap1 stop**.

Step 13

To copy the files, navigate to **Administration > File Management > File Directory**.

▼ Administration 1

System Settings

Console Settings

Stack Management

Bluetooth Settings

User Accounts

Idle Session Timeout

▶ Time Settings

Step 14

The default *Flash* is available. Alternatively, you can select *USB* from the *Drive* drop-down menu.

File Directory

Auto Mirror Configuration: ☒ Enable

File Table

Free Space: 163144/305484 KB

Drive:

Flash ▾

Flash
USB

Go

File Name

Permissions

system

Conclusion

Now you know all about ISE and how to configure CoA in the Catalyst 1300 series switches.

For more information, check out the video below.

View a video related to this article...

[Click here to view other Tech Talks from Cisco](#)