

Configure Device Authorization Control (DAC) Management through Smart Network Application (SNA)

Objective

The Smart Network Application (SNA) system displays an overview of the network topology including detailed monitoring information for devices and traffic. SNA enables viewing and modifying of configurations globally on all supported devices in the network.

SNA has a feature known as the Device Authorization Control (DAC) that allows you to configure a list of authorized client devices in the network. DAC activates 802.1X features on SNA devices in the network and an embedded Remote Authentication Dial-In User Service (RADIUS) or RADIUS Host Server can be configured on one of the SNA devices. DAC is done via Media Access Control (MAC) authentication.

This article provides instructions on how to configure the DAC Management through SNA.

Applicable Devices

- Sx350 Series
- SG350X Series
- Sx550X Series

Note: Devices from the Sx250 Series can provide SNA information when they are connected to the network, but SNA cannot be launched from these devices.

Software Version

- 2.2.5.68

DAC Workflow

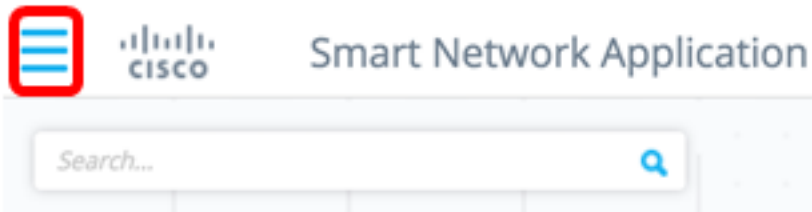
You can configure DAC management through the following steps:

- [Activate DAC](#)
- [Configure RADIUS Server and Clients](#)
- [DAC List Management](#)

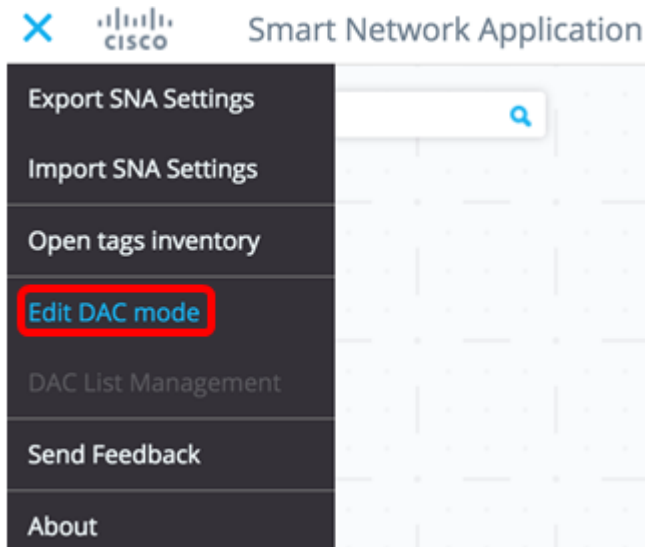
[Activate DAC](#)

To access and activate DAC, follow these steps:

Step 1. Click the **Options** menu on the upper-left corner of the SNA page to show available options.



Step 2. Choose **Edit DAC mode**.



DAC Edit Mode is now activated. You should see the blue frame below the topology map and the control panel on the bottom of the screen.



Step 3. (Optional) To exit DAC Edit Mode, click the **Exit** button.

[Configure RADIUS Server and Clients](#)

Step 1. In the Topology view, choose one of the SNA devices and click on its **Options** menu.



Step 2. Click **+ Set as DAC server**.



Step 3. If the device has more than a single IP address, choose one of those addresses as the one to be used by DAC. In this example, 192.168.1.127 | Static is chosen.

< BACK

Select IP Address

switche6f4d3 / fec0::42a6:e8ff:fee6:f4d3

IP ADDRESS

fec0::42a6:e8ff:fee6:f4d3 | Dynamic

127.0.0.1 | Static unstable connection

192.168.1.127 | Static

fec0::42a6:e8ff:fee6:f4d3 | Dynamic

fe80::42a6:e8ff:fee6:f4d3 | Dynamic

ff02::1 | Dynamic

Note: The list of addresses indicates whether the IP interface is static or dynamic. You will be warned that choosing a dynamic IP might cause unstable connection.

Select IP Address

switche6f4d3 / fec0::42a6:e8ff:fee6:f4d3

IP ADDRESS

192.168.1.127 | Dynamic

⚠ Dynamic ip might cause an unstable connection

DONE

Step 4. Click **DONE**.

< BACK

Select IP Address

switche6f4d3 / fec0::42a6:e8ff:fee6:f4d3

IP ADDRESS

DONE

Note: When editing an existing DAC server, the address currently used by its clients is pre-selected.

The DAC RADIUS server is highlighted in solid in the Topology view.



Step 5. Choose one of the SNA devices and click on its Options menu.

Note: If no clients are selected, you will be unable to apply the settings.

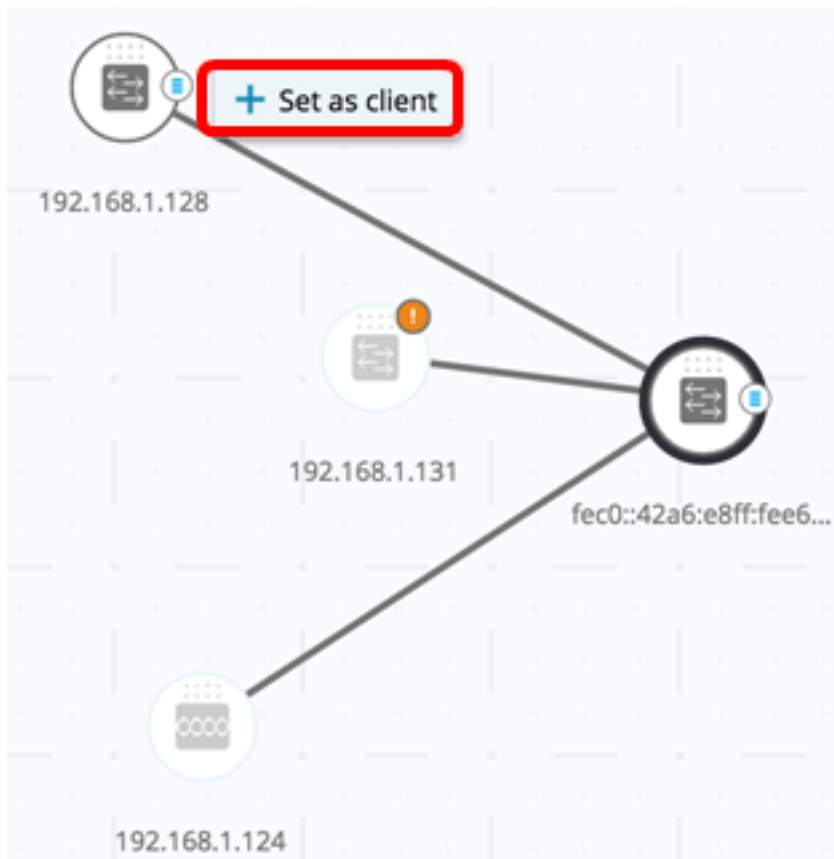


If a switch is already a client of the DAC RADIUS server, its IP address is in the NAS table of the RADIUS server and the RADIUS server is configured in its RADIUS server table with usage type 802.1X or all in priority 0. This switch is pre-selected.

If a client is chosen, which already has a RADIUS server configured for 802.1X other than the previously selected server, you will be notified that the proceedings will interrupt the existing RADIUS server operation.

If a client is chosen, which has a RADIUS server configured for 802.1X in priority 0 other than the previously-selected server, an error message is displayed and DAC is not configured on this client.

Step 6. Click + **Set as client**.



Step 7. Check the check box or check boxes of the port or ports from the client switch to apply 802.1X authentications.

Note: In this example, GE1/1, GE1/2, GE1/3, and GE1/4 ports are checked.

< BACK

DONE

Select Client Ports

switche6fa9f / 192.168.1.128

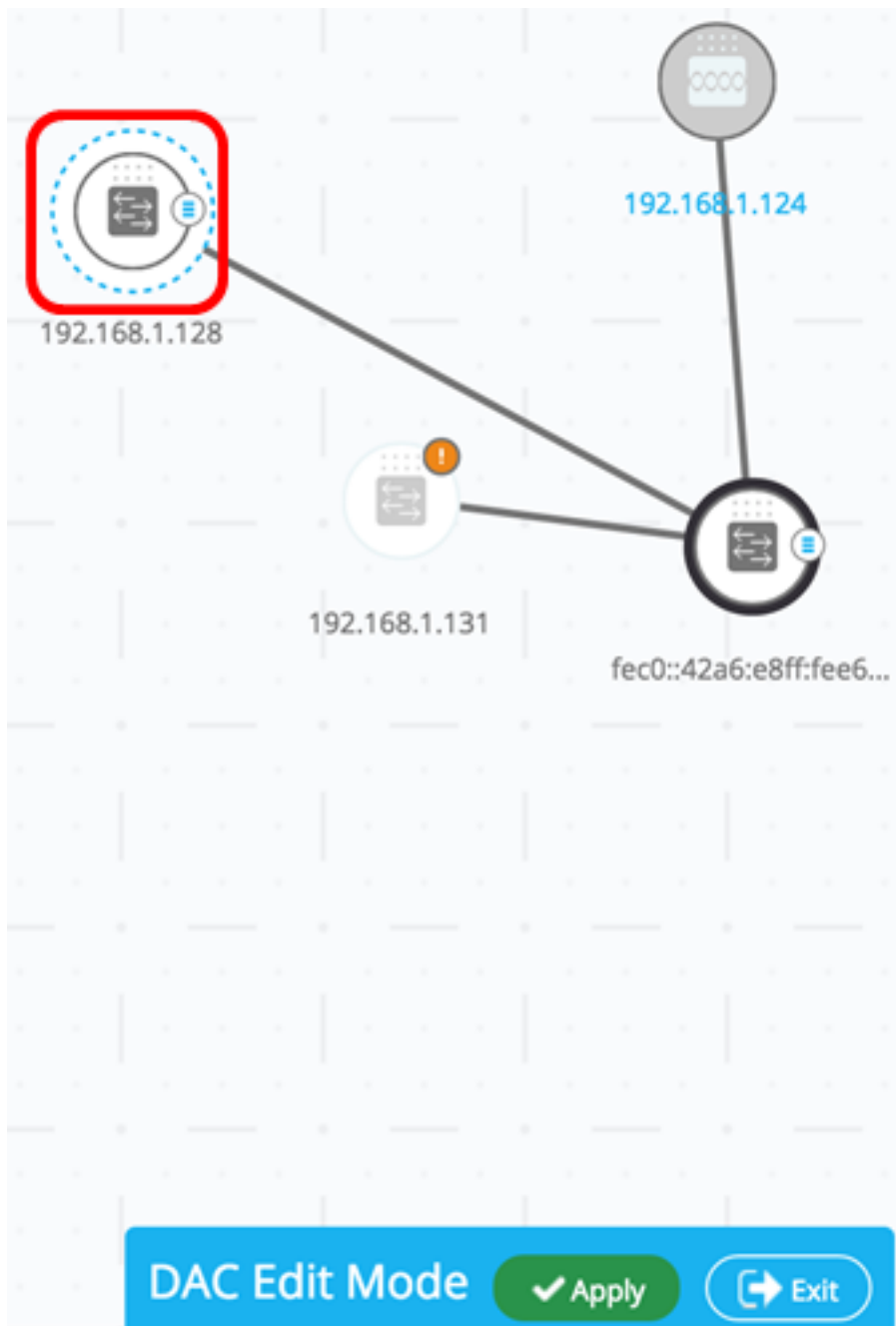
★ Select Recommended

<input type="checkbox"/>	PORT	SWITCHPORT MODE	DESCRIPTION	RECOMMENDED
<input checked="" type="checkbox"/>	GE1/1	trunk		
<input checked="" type="checkbox"/>	GE1/2	access		★
<input checked="" type="checkbox"/>	GE1/3	access		★
<input checked="" type="checkbox"/>	GE1/4	access		★
<input type="checkbox"/>	GE1/5	trunk		★

Note: The SNA recommends a list of all edge ports or all the ports that are not known to be connected to other switches or clouds.

Step 8. (Optional) Click the **Select Recommended** button to check all recommended ports.

Step 9. Click **DONE**. The DAC RADIUS client is highlighted in dashed blue in the Topology view.



Step 10. Click **Apply** to save the changes.

Step 11. Enter a Keystring that will be used by the DAC RADIUS server with all its clients on the network.

Apply

STEP 1 - Insert Keystring » STEP 2 - Review Changes » STEP 3 - Apply Changes

i Please notice: you must enter a manual keystring or choose the auto generated option

Manual Auto Generated

Cisco1234|

Note: In this example, Cisco1234 is used.

Step 12. (Optional) Toggle the button to **Auto Generated** to use an auto-generated Keystring.

Apply

STEP 1 - Insert Keystring » STEP 2 - Review Changes » STEP 3 - Apply Changes

i Please notice: you must enter a manual keystring or choose the auto generated option

Manual Auto Generated

An auto generated Keystring will be created by the system

Step 13. Click **Continue** on the upper-right hand corner of the page.

CONTINUE

Step 14. Review the changes then click **APPLY CHANGES**.

Apply ×

STEP 1 - Insert Keystring » STEP 2 - Review Changes » STEP 3 - Apply Changes **APPLY CHANGES**
 Save to Startup configuration

SWITCH	ACTIONS
switche6f4d3 fec0:42a6:e8ff:fee6:f4d3	Set radius server fec0:42a6:e8ff:fee6:f4d3
switche6fa9f 192.168.1.128	Add radius client 192.168.1.128 to server fec0:42a6:e8ff:fee6:f4d3
switche6fa9f 192.168.1.128	Set radius client for 192.168.1.128

Step 15. (Optional) Uncheck the **Save to startup configuration** check box if you do not wish to save the settings in the configuration file.

APPLY CHANGES
 Save to startup configuration

Step 16. (Optional) If you are using a Read Only account, you may be prompted to enter your credentials to continue. Enter the password in the *Password* field then click **SUBMIT**.

Upgrade Access Permission X



SESSION IS IN READ ONLY MODE
Enter your password to upgrade permission and continue

Username:

cisco

Password:

SUBMIT

Step 17. The Status column should contain green check boxes that confirm successful application of changes. Click **DONE**.

Apply

STEP 1 - Insert Keystring » STEP 2 - Review Changes » STEP 3 - Apply Changes

DONE

Save to startup configuration

SWITCH	ACTIONS	STATUS
switche6f4d3 fec0:42a6:e8ff:fee6:f4d3	Set radius server fec0:42a6:e8ff:fee6:f4d3	✔ Set radius server fec0:42a6:e8ff:fee6:f4d3 succeed...
switche6fa9f 192.168.1.128	Add radius client 192.168.1.128 to server fec0:42a6:e8ff:fee6:f4d3	✔ Add DAC client 192.168.1.128 to server fec0:42a6:...
switche6fa9f 192.168.1.128	Set radius client for 192.168.1.128	✔ DAC configuration for client 192.168.1.128 succeed...

After the DAC is configured, an alert is displayed whenever a new non-blocklisted device is rejected on the network through a DAC-enabled RADIUS server. You will be asked whether to add this device to the allow list of authorized devices, or send it into a block list so that you are not alerted again.

When informing the user of the new device, SNA provides the MAC address of the device and the port which the device attempted to access the network.

If a rejection event is received from a device that is not a DAC RADIUS server, the message is ignored, and all further messages from this device for the next 20 minutes are ignored. After 20 minutes, SNA checks again if the device is a DAC RADIUS server. If a user is added to the allow list, the device is added to the DAC group of all DAC servers. When this configuration is saved, you can choose whether to save this setting immediately to the startup configuration of the server. This option is selected by default.

Until a device is added to the allow list, it is not allowed access to the network. You can view

and change the allow and block lists at any time, as long as a DAC RADIUS server is defined and reachable. To configure the DAC List Management, skip to [DAC List Management](#).

When applying the DAC settings, you are presented with a report listing actions that will be applied to the participating devices. After you approve the changes, you can decide if the settings should additionally be copied to the startup configuration file of the configured devices. Finally, apply the configurations.

The report displays warnings if some steps of the DAC configuration process are missed, along with the status of the actions as handled by the devices.

Field	Value	Comments
Device	The device identifiers (Host name or IP address)	
Action	<p>Possible actions for DAC server:</p> <ul style="list-style-type: none"> • Enable RADIUS server • Disable RADIUS server • Update client list • Create RADIUS server group • Delete RADIUS server group <p>Possible actions for DAC client:</p> <ul style="list-style-type: none"> • Add RADIUS server connection • Update RADIUS server connection • Remove RADIUS server connection • Update 802.1x settings • Update interface authentication settings • Update interface host and session settings 	It is possible (and likely) for multiple actions to appear for each device. Each action can have its own status.
Warnings	<p>Possible warnings for DAC server include:</p> <ul style="list-style-type: none"> • Selected IP interface is dynamic. <p>Possible warnings for DAC clients include:</p> <ul style="list-style-type: none"> • Device is already a client of a different RADIUS server. • No ports are selected. 	Warnings also contain links to the sections of the DAC where they can be addressed. Changes can be applied when warnings are present.
Status	<ul style="list-style-type: none"> • Pending • Success • Failure 	When the status is a failure, the error message is shown for the action.

DAC List Management

Once you have added client devices and selected which of their ports are to be authenticated, all unauthenticated devices detected on those ports are added to the list of Unauthenticated Devices.

DAC supports the following lists of devices:

- Allow List — Contains the list of all clients that can be authenticated.
- Block List — **Contains** the list of clients that must never be authenticated.

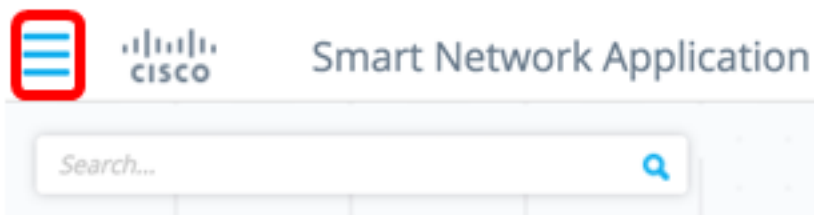
If you want devices and their ports to be authenticated, they must be added to the allow lists. If you do not want them to be authenticated, no action is required as they will be added to the block list by default.

[See glossary for additional information.](#)

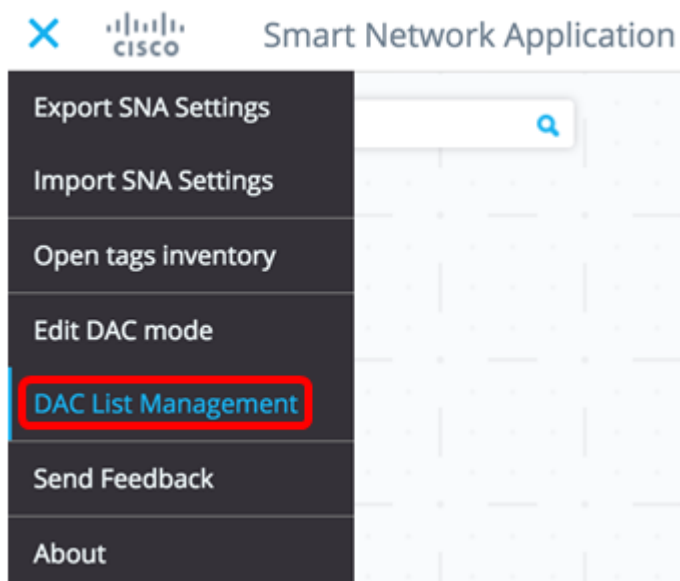
Add Devices to Allow list or Block list

To add devices to the allow list or block list, follow these steps:

Step 1. Click the **Options** menu on the upper-left corner of the SNA page to show available options.



Step 2. Choose **DAC List Management**.



Step 3. Click the **UNAUTHENTICATED DEVICES** tab. This page will display the list of all unauthenticated devices.

DAC List Management

WHITELIST

BLACKLIST

UNAUTHENTICATED DEVICES 2

 Select one device or more from the list and then click on an action of your choice

Save to startup configuration

Note: Alternatively, you can click the DAC List Management System icon at the upper-right corner of the SNA page.



Step 4. (Optional) Check the check box next to the MAC address of the device or devices that you want to add to the allow list and click **Add to Allow list**.

DAC List Management

WHITELIST

BLACKLIST

UNAUTHENTICATED DEVICES 2

 Select one device or more from the list and then click on an action of your choice

Save to startup configuration

Add to Whitelist Add to Blacklist Dismiss

<input type="checkbox"/>	MAC ADDRESS	CONNECTING SWITCH	CONNECTING PORT	LAST SEEN	STATUS
<input checked="" type="checkbox"/>	0C:27:24:1F:47:A8	192.168.1.128	gi1/0/3	November 22nd 2016, 12:11:01 pm	Pending
<input type="checkbox"/>	0C:27:24:1F:47:A9	192.168.1.128	gi1/0/3	November 22nd 2016, 12:08:11 pm	Pending

Step 5. (Optional) Check the check box next to the MAC address of the device or devices that you want to add to the block list and click **Add to Block list**.

DAC List Management

WHITELIST BLACKLIST UNAUTHENTICATED DEVICES 1

Select one device or more from the list and then click on an action of your choice

Save to startup configuration

Add to Whitelist Add to Blacklist Dismiss

<input type="checkbox"/>	MAC ADDRESS	CONNECTING SWITCH	CONNECTING PORT	LAST SEEN	STATUS
<input checked="" type="checkbox"/>	0C:27:24:1F:47:A9	192.168.1.128	gi1/0/3	November 22nd 2016, 12:15:12 pm	Pending
<input type="checkbox"/>	0C:27:24:1F:47:A8	192.168.1.128	gi1/0/3	November 22nd 2016, 12:15:01 pm	success

Step 6. (Optional) Check the check box next to the MAC address of the device or devices that you want to dismiss and click **Dismiss**.

DAC List Management

WHITELIST BLACKLIST UNAUTHENTICATED DEVICES 1

Select one device or more from the list and then click on an action of your choice

Save to startup configuration

Add to Whitelist Add to Blacklist Dismiss

<input checked="" type="checkbox"/>	MAC ADDRESS	CONNECTING SWITCH	CONNECTING PORT	LAST SEEN	STATUS
<input checked="" type="checkbox"/>	00:41:D2:A0:FA:20	192.168.1.128	gi1/0/5	November 22nd 2016, 12:34:14 pm	Pending

Note: All packets entering on the ports on the device are authenticated on the RADIUS server.

You should now have added a device to the Allow list or Block list.

Manage Devices on Allow list or Block list

To manage the allow or block lists, click the **ALLOW LIST** or **BLOCK LIST** tab accordingly.

DAC List Management

WHITELIST **BLACKLIST** UNAUTHENTICATED DEVICES


i Select one device or more from the list and then click on an action of your choice

Save to startup configuration Add Device

MAC ADDRESS LAST SEEN

<input type="checkbox"/>	00:41:D2:A0:FA:20
--------------------------	-------------------

You can perform the following tasks in these pages:

- Remove from list — This action removes the chosen device or devices from the list.
- Move to Block list or Move to Allow list — This action moves the chosen device or devices to the specified list.
- Add a device — This action adds a device to either the block or allow list by entering its MAC address and clicking the **ADD+** button.
- Search a device using MAC address — Enter a MAC address and click the **Search**  button.

You should now have managed the devices on the DAC list.