

Configuración de la gestión del control de autorización de dispositivos (DAC) a través de Smart Network Application (SNA)

Objetivo

El sistema Smart Network Application (SNA) muestra una descripción general de la topología de red, incluida información de supervisión detallada para dispositivos y tráfico. SNA permite ver y modificar configuraciones globalmente en todos los dispositivos compatibles de la red.

SNA tiene una función conocida como Control de autorización de dispositivos (DAC) que permite configurar una lista de dispositivos cliente autorizados en la red. DAC activa las funciones 802.1X en los dispositivos SNA de la red y se puede configurar un servicio de usuario de acceso telefónico de autenticación remota (RADIUS) o un servidor host RADIUS integrado en uno de los dispositivos SNA. El DAC se realiza mediante la autenticación de control de acceso a medios (MAC).

En este artículo se proporcionan instrucciones sobre cómo configurar DAC Management a través de SNA.

Dispositivos aplicables

- Serie Sx350
- Serie SG350X
- Serie Sx550X

Nota: Los dispositivos de la serie Sx250 pueden proporcionar información SNA cuando se conectan a la red, pero SNA no se puede iniciar desde estos dispositivos.

Versión del software

- 2.2.5.68

Flujo de trabajo de DAC

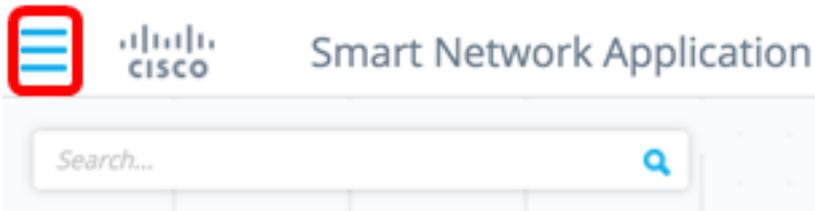
Puede configurar la administración de DAC mediante los siguientes pasos:

- [Activar DAC](#)
- [Configuración del servidor RADIUS y los clientes](#)
- [Administración de listas DAC](#)

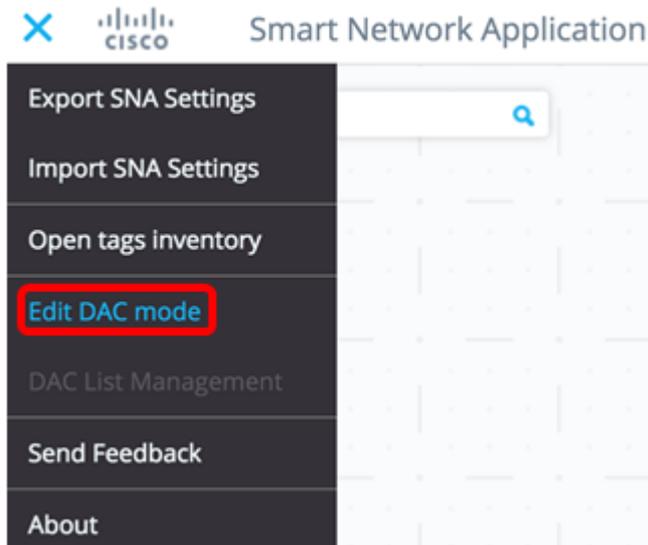
[Activar DAC](#)

Para acceder y activar DAC, siga estos pasos:

Paso 1. Haga clic en el menú **Opciones** de la esquina superior izquierda de la página SNA para mostrar las opciones disponibles.



Paso 2. Elija **Editar modo DAC**.



El modo de edición DAC ya está activado. Debería ver la trama azul debajo del mapa de topología y el panel de control en la parte inferior de la pantalla.



Paso 3. (Opcional) Para salir del modo de edición DAC, haga clic en el botón **Salir**.

[Configuración del servidor RADIUS y los clientes](#)

Paso 1. En la vista Topología, elija uno de los dispositivos SNA y haga clic en su menú **Opciones**.



Paso 2. Haga clic en **+ Establecer como servidor DAC**.



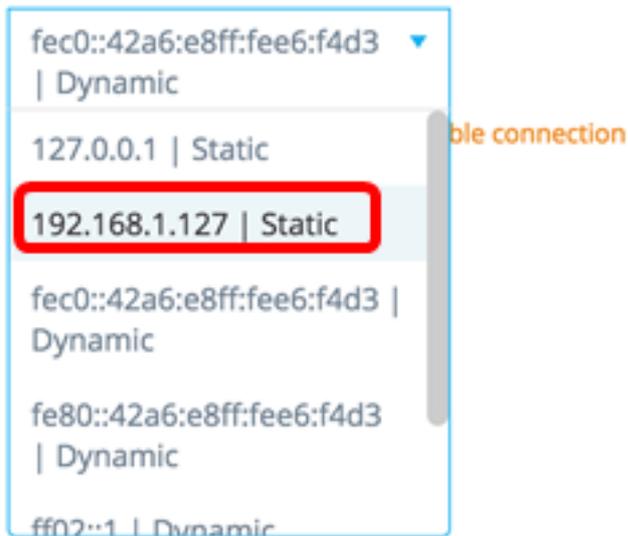
Paso 3. Si el dispositivo tiene más de una sola dirección IP, elija una de esas direcciones como la que utilizará DAC. En este ejemplo, 192.168.1.127 | Estático.

< BACK

Select IP Address

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

IP ADDRESS



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

127.0.0.1 | Static

192.168.1.127 | Static

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

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

ff02::1 | Dynamic

unstable connection

Nota: La lista de direcciones indica si la interfaz IP es estática o dinámica. Se le advertirá de que elegir una IP dinámica puede provocar una conexión inestable.

Select IP Address

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

IP ADDRESS



192.168.1.127 | Dynamic

⚠ Dynamic ip might cause an unstable connection

DONE

Paso 4. Haga clic en Done (Listo).

< BACK

Select IP Address

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

IP ADDRESS

DONE

Nota: Al editar un servidor DAC existente, se preselecciona la dirección que utilizan actualmente sus clientes.

El servidor RADIUS DAC se resalta en sólido en la vista Topología.



Paso 5. Elija uno de los dispositivos SNA y haga clic en su menú Opciones.

Nota: Si no se selecciona ningún cliente, no podrá aplicar la configuración.

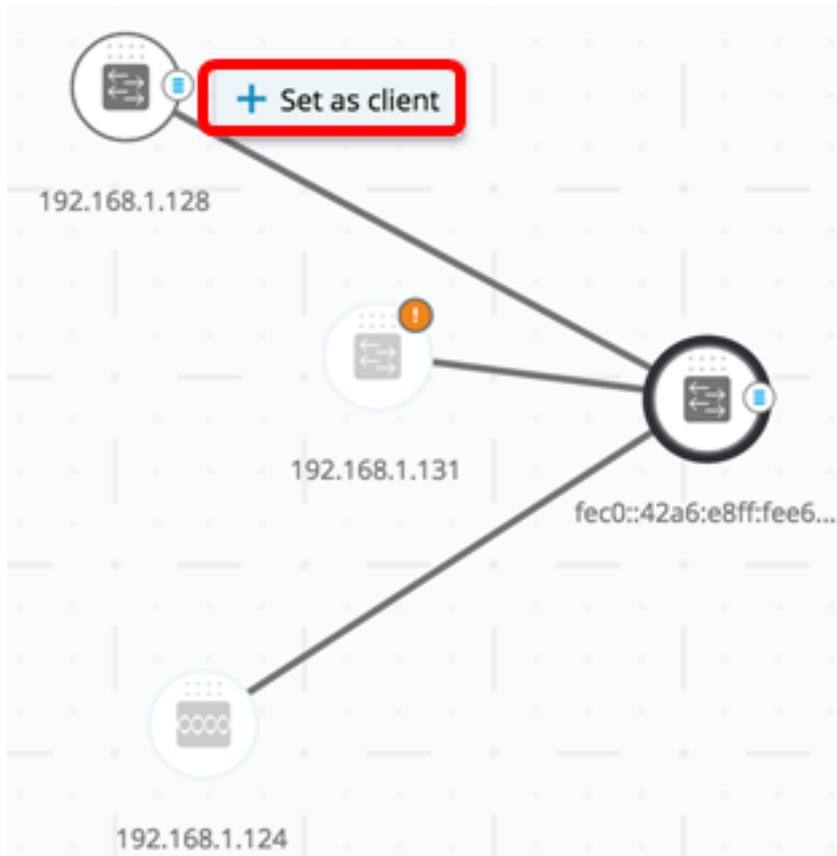


Si un switch ya es cliente del servidor RADIUS DAC, su dirección IP está en la tabla NAS del servidor RADIUS y el servidor RADIUS está configurado en su tabla de servidor RADIUS con el tipo de uso 802.1X o todos en la prioridad 0. Este switch está preseleccionado.

Si se elige un cliente, que ya tiene un servidor RADIUS configurado para 802.1X que no sea el servidor seleccionado anteriormente, se le notificará que el procedimiento interrumpirá la operación del servidor RADIUS existente.

Si se elige un cliente, que tiene un servidor RADIUS configurado para 802.1X en la prioridad 0 diferente del servidor seleccionado anteriormente, se muestra un mensaje de error y DAC no se configura en este cliente.

Paso 6. Haga clic en + **Establecer como cliente**.



Paso 7. Marque la casilla de verificación o casillas de verificación del puerto o puertos del switch cliente para aplicar las autenticaciones 802.1X.

Nota: En este ejemplo, se verifican los puertos GE1/1, GE1/2, GE1/3 y GE1/4.

< BACK

DONE

Select Client Ports

switche6fa9f / 192.168.1.128

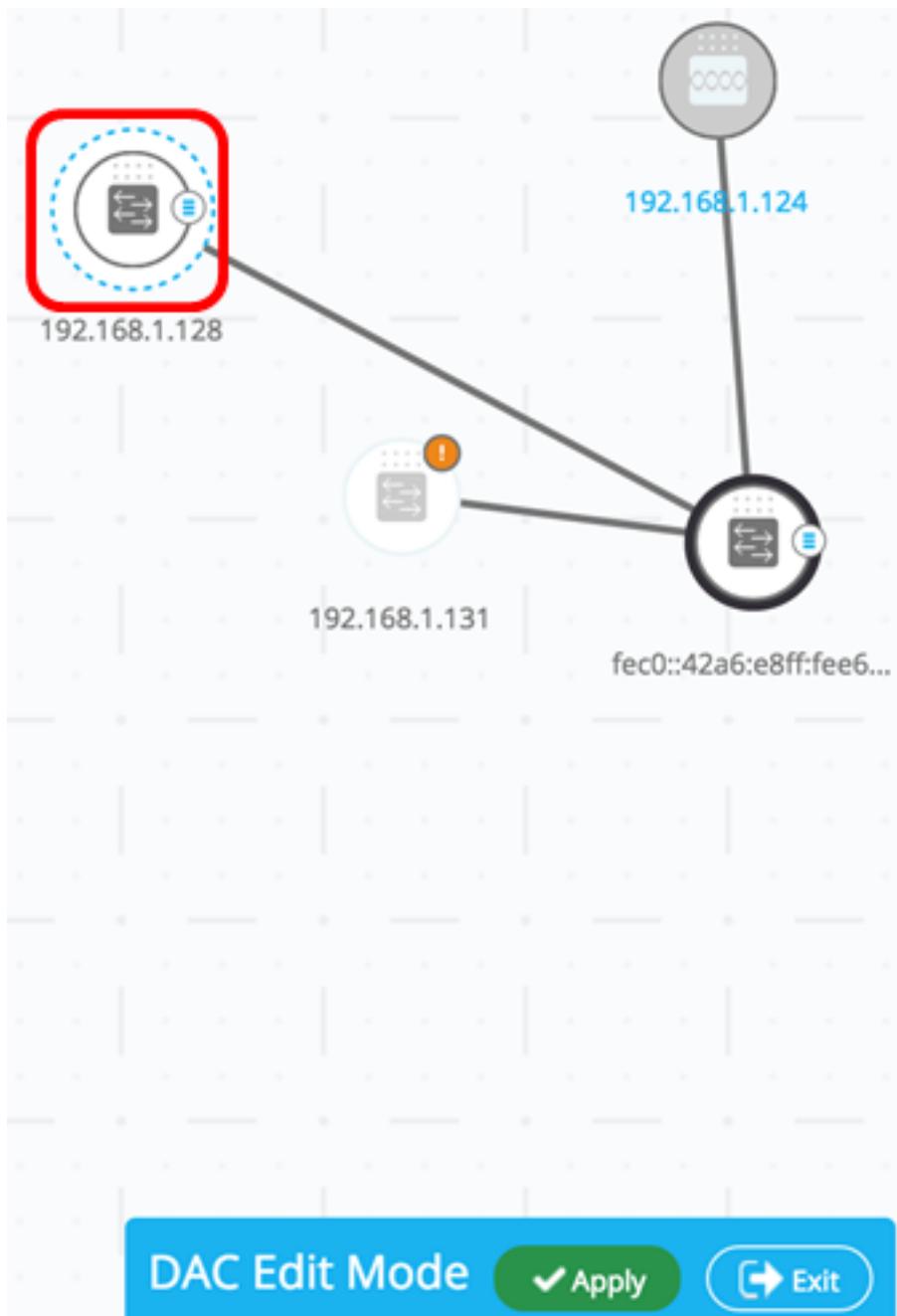
★ Select Recommended

<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		★

Nota: El SNA recomienda una lista de todos los puertos de borde o de todos los puertos que no se sabe que están conectados a otros switches o nubes.

Paso 8. (Opcional) Haga clic en el botón **Seleccionar recomendado** para verificar todos los puertos recomendados.

Paso 9. Haga clic en Done (Listo). El cliente DAC RADIUS se resalta en azul discontinuo en la vista Topología.



Paso 10. Haga clic en **Aplicar** para guardar los cambios.

Paso 11. Introduzca una cadena de clave que utilizará el servidor RADIUS DAC con todos sus clientes en la red.

Apply

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

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

Manual Auto Generated

Cisco1234|

Nota: En este ejemplo, se utiliza Cisco1234.

Paso 12. (Opcional) Cambie el botón a **Generado automáticamente** para utilizar una cadena de clave generada automáticamente.

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

Paso 13. Haga clic en **Continuar** en la esquina superior derecha de la página.

CONTINUE

Paso 14. Revise los cambios y haga clic en **APLICAR CAMBIOS**.

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

Paso 15. (Opcional) Desmarque la casilla de verificación **Guardar en la configuración de inicio** si no desea guardar la configuración en el archivo de configuración.

APPLY CHANGES
 Save to startup configuration

Paso 16. (Opcional) Si utiliza una cuenta de sólo lectura, se le puede solicitar que introduzca sus credenciales para continuar. Ingrese la contraseña en el campo *Password* y luego haga clic en **SUBMIT**.

Upgrade Access Permission X



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

Username:

cisco

Password:

SUBMIT

Paso 17. La columna Estado debe contener casillas de verificación verdes que confirmen la correcta aplicación de los cambios. Haga clic en Done (Listo).

Apply

STEP 1 - Insert Keysting » 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 succee...
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...

Después de configurar el DAC, se muestra una alerta cada vez que se rechaza un nuevo dispositivo no incluido en la lista de bloqueo en la red a través de un servidor RADIUS habilitado para DAC. Se le preguntará si desea agregar este dispositivo a la lista de dispositivos autorizados para permitir o enviarlo a una lista de bloqueo para que no reciba una nueva alerta.

Al informar al usuario del nuevo dispositivo, SNA proporciona la dirección MAC del dispositivo y el puerto al que el dispositivo intentó acceder a la red.

Si se recibe un evento de rechazo de un dispositivo que no es un servidor RADIUS DAC, se omite el mensaje y se ignoran todos los mensajes adicionales de este dispositivo durante los próximos 20 minutos. Después de 20 minutos, SNA verifica de nuevo si el dispositivo es un servidor RADIUS DAC. Si se agrega un usuario a la lista de permitidos, el dispositivo se agrega al grupo DAC de todos los servidores DAC. Cuando se guarda esta configuración, puede elegir si guardar esta configuración inmediatamente en la configuración de inicio del servidor. Esta opción está seleccionada de forma predeterminada.

Hasta que no se agregue un dispositivo a la lista de permitidos, no se le permite el acceso a la red. Puede ver y cambiar las listas de permitidos y bloqueados en cualquier momento, siempre y cuando se defina y alcance un servidor RADIUS DAC. Para configurar la Administración de lista DAC, vaya directamente a [Administración de lista DAC](#).

Al aplicar la configuración de DAC, se le presenta un informe que enumera las acciones que se aplicarán a los dispositivos participantes. Después de aprobar los cambios, puede decidir si los ajustes se deben copiar adicionalmente al archivo de configuración de inicio de los dispositivos configurados. Por último, aplique las configuraciones.

El informe muestra advertencias si no se cumplen algunos pasos del proceso de configuración de DAC, junto con el estado de las acciones tal como las manejan los dispositivos.

Campo	Valor	Comentarios
Dispositivo	Identificadores de dispositivo (nombre de host o dirección IP)	
Acción	<p>Acciones posibles para el servidor DAC:</p> <ul style="list-style-type: none"> • Activar servidor RADIUS • Deshabilitar servidor RADIUS • Actualizar lista de clientes • Crear grupo de servidores RADIUS • Eliminar grupo de servidores RADIUS <p>Acciones posibles para el cliente DAC:</p> <ul style="list-style-type: none"> • Agregar conexión del servidor RADIUS • Actualizar conexión del servidor RADIUS • Eliminar conexión del servidor RADIUS • Actualizar configuración 802.1x • Actualizar configuración de autenticación de la interfaz • Actualizar la configuración del host de la interfaz y de la sesión 	<p>Es posible (y probable) que aparezcan varias acciones para cada dispositivo. Cada acción puede tener su propio estado.</p>
Advertencias	<p>Las advertencias posibles para el servidor DAC incluyen:</p> <ul style="list-style-type: none"> • La interfaz IP 	<p>Las advertencias también contienen enlaces a las secciones del CAD en las que se pueden abordar.</p>

	<p>seleccionada es dinámica.</p> <p>Entre las posibles advertencias para los clientes DAC se incluyen:</p> <ul style="list-style-type: none"> • El dispositivo ya es cliente de un servidor RADIUS diferente. • No hay puertos seleccionados. 	<p>Los cambios se pueden aplicar cuando hay advertencias.</p>
Estado	<ul style="list-style-type: none"> • Pendiente • Éxito • Falla 	<p>Cuando el estado es una falla, se muestra el mensaje de error para la acción.</p>

Administración de listas DAC

Una vez que haya agregado los dispositivos cliente y haya seleccionado cuáles de sus puertos se autenticarán, todos los dispositivos no autenticados detectados en esos puertos se agregarán a la lista de dispositivos no autenticados.

DAC admite las siguientes listas de dispositivos:

- Permitir lista: contiene la lista de todos los clientes que se pueden autenticar.
- Lista de bloqueo: **Contiene** la lista de clientes que nunca se deben autenticar.

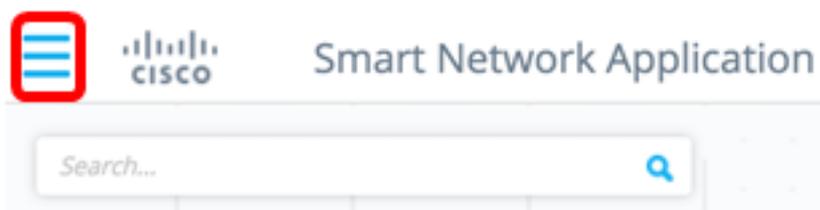
Si desea que los dispositivos y sus puertos se autenticen, deben agregarse a las listas de permitidos. Si no desea que se autenticen, no se requiere ninguna acción, ya que se agregarán a la lista de bloqueo de forma predeterminada.

[Consulte el glosario para obtener información adicional.](#)

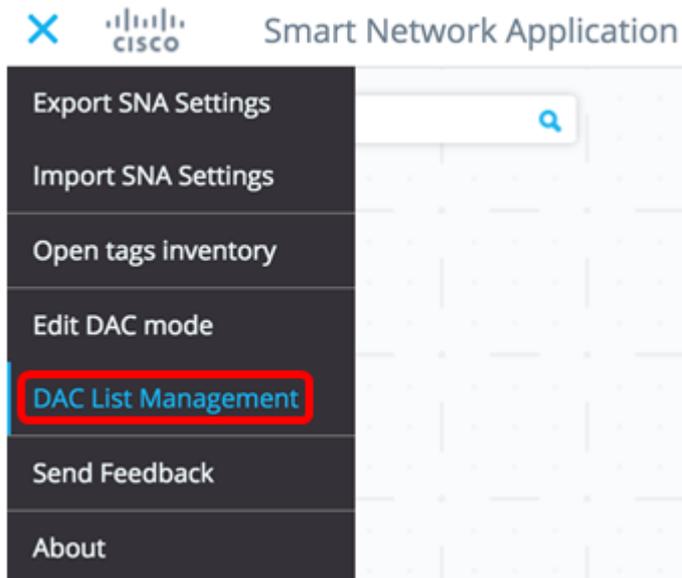
Agregar dispositivos a la lista Permitir o a la lista Bloquear

Para agregar dispositivos a la lista de permitidos o de bloqueo, siga estos pasos:

Paso 1. Haga clic en el menú **Opciones** de la esquina superior izquierda de la página SNA para mostrar las opciones disponibles.

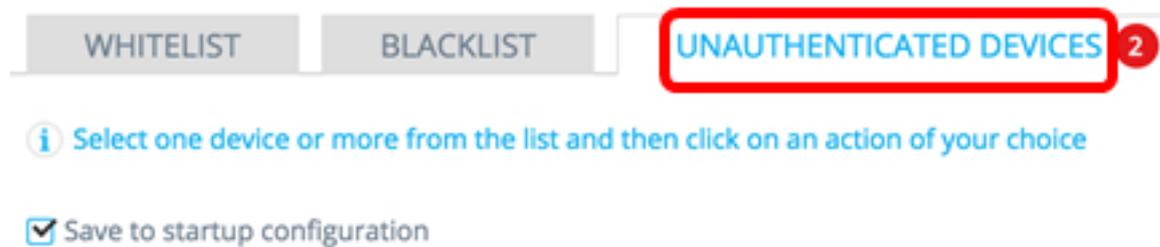


Paso 2. Elija **Administración de lista DAC**.



Paso 3. Haga clic en la pestaña **DISPOSITIVOS NO AUTENTICADOS**. Esta página mostrará la lista de todos los dispositivos no autenticados.

DAC List Management



Nota: De manera alternativa, puede hacer clic en el icono del sistema de administración de listas DAC en la esquina superior derecha de la página SNA.



Paso 4. (Opcional) Marque la casilla de verificación junto a la dirección MAC del dispositivo o dispositivos que desea agregar a la lista de permitidos y haga clic en **Agregar a la lista Permitir**.

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

Paso 5. (Opcional) Marque la casilla de verificación junto a la dirección MAC del dispositivo o dispositivos que desea agregar a la lista de bloqueo y haga clic en **Agregar a la lista de bloqueo**.

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

Paso 6. (Opcional) Marque la casilla de verificación junto a la dirección MAC del dispositivo o dispositivos que desea descartar y haga clic en **Descartar**.

DAC List Management

WHITELIST BLACKLIST **UNAUTHENTICATED DEVICES** 1

i 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

Nota: Todos los paquetes que ingresan en los puertos del dispositivo se autentican en el servidor RADIUS.

Ahora debería haber agregado un dispositivo a la lista Permitir o Bloquear.

Administrar dispositivos en la lista Permitir o en la lista Bloquear

Para administrar las listas de permitidos o bloqueados, haga clic en la pestaña **ALLOW LIST** o **BLOCK LIST** en consecuencia.

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

Remove from list Move to Whitelist **ADD +**

<input type="checkbox"/>	MAC ADDRESS	LAST SEEN
<input type="checkbox"/>	00:41:D2:A0:FA:20	

Puede realizar las tareas siguientes en estas páginas:

- Eliminar de la lista: esta acción elimina el dispositivo o dispositivos seleccionados de la lista.
- Mover a la lista Bloquear o Mover a la lista Permitir: esta acción mueve el dispositivo o

dispositivos seleccionados a la lista especificada.

- Agregar un dispositivo: esta acción agrega un dispositivo al bloque o a la lista de permitidos ingresando su dirección MAC y haciendo clic en el **botón ADD+**.
- Buscar un dispositivo mediante la dirección MAC: introduzca una dirección MAC y haga clic en el botón **Buscar**  para abrir el Navegador.

Ahora debería haber administrado los dispositivos de la lista DAC.