

通过智能网络应用(SNA)配置设备授权控制(DAC)管理

目标

智能网络应用(SNA)系统显示网络拓扑概述，包括设备和流量的详细监控信息。SNA允许全局查看和修改网络中所有受支持设备上的配置。

SNA具有一种称为设备授权控制(DAC)的功能，允许您配置网络中的授权客户端设备列表。DAC在网络中的SNA设备上激活802.1X功能，并且可以在其中一个SNA设备上配置嵌入式远程身份验证拨入用户服务(RADIUS)或RADIUS主机服务器。DAC通过介质访问控制(MAC)身份验证完成。

本文提供了如何通过SNA配置DAC管理的说明。

适用设备

- Sx350 系列
- SG350X 系列
- Sx550X 系列

注意：当Sx250系列的设备连接到网络时，它们可以提供SNA信息，但SNA无法从这些设备启动。

软件版本

- 2.2.5.68

DAC工作流程

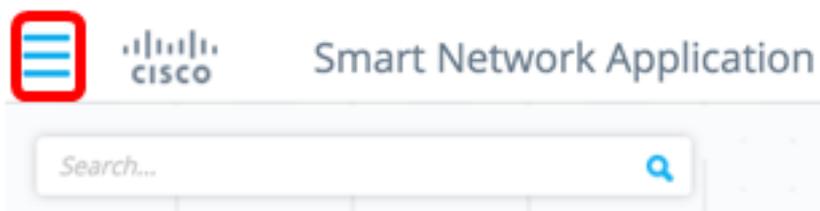
您可以通过以下步骤配置DAC管理：

- [激活DAC](#)
- [配置RADIUS服务器和客户端](#)
- [DAC列表管理](#)

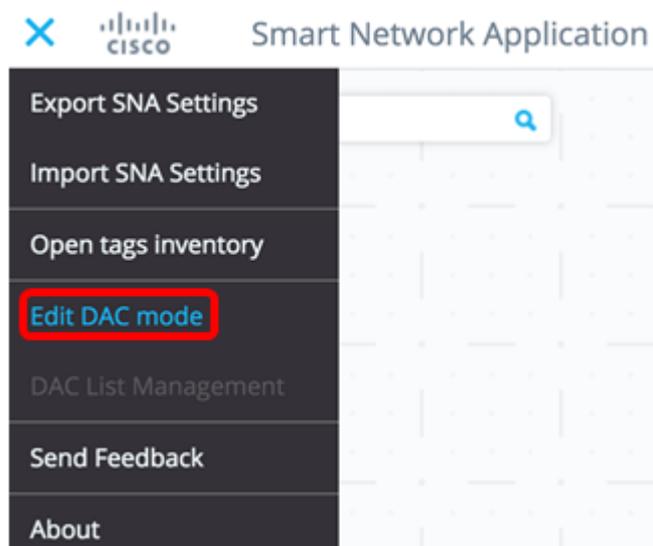
[激活DAC](#)

要访问并激活DAC，请执行以下步骤：

步骤1.单击SNA页左上角的**Options**菜单以显示可用选项。



步骤2.选择“编辑DAC模式”。



DAC编辑模式现在已激活。您应该看到拓扑图下方的蓝色帧和屏幕底部的控制面板。



步骤3. (可选) 要退出DAC编辑模式，请单击“退出”按钮。

配置RADIUS服务器和客户端

步骤1.在“拓扑”视图中，选择SNA设备之一，然后单击其“选项”菜单。



步骤2.单击+ Set as DAC server。



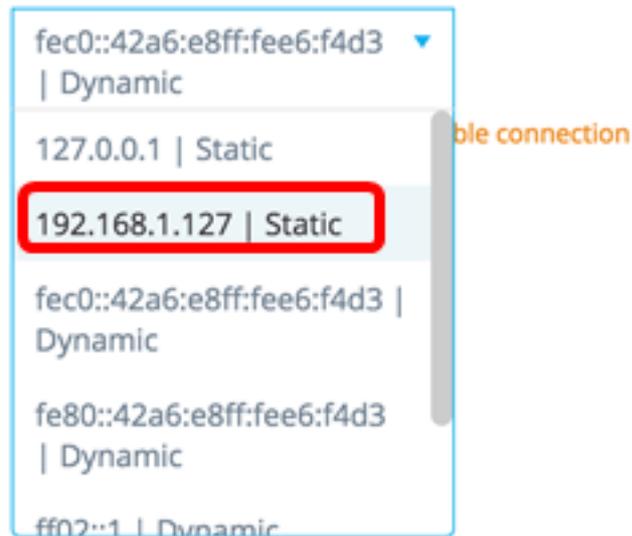
步骤3.如果设备有多个IP地址，请选择其中一个地址作为DAC使用的地址。在本例中，192.168.1.127 |选择静态。

< 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

注意：地址列表指示IP接口是静态接口还是动态接口。系统将警告您，选择动态IP可能导致连接不稳定。

Select IP Address

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

IP ADDRESS



192.168.1.127	Dynamic
---------------	---------

⚠ Dynamic ip might cause an unstable connection

DONE

步骤4.单击“完成”。

< BACK

Select IP Address

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

IP ADDRESS

DONE

注意：编辑现有DAC服务器时，会预先选择其客户端当前使用的地址。

DAC RADIUS服务器在拓扑视图中以实体突出显示。



步骤5.选择SNA设备之一，然后单击其“选项”菜单。

注意：如果未选择客户端，您将无法应用设置。

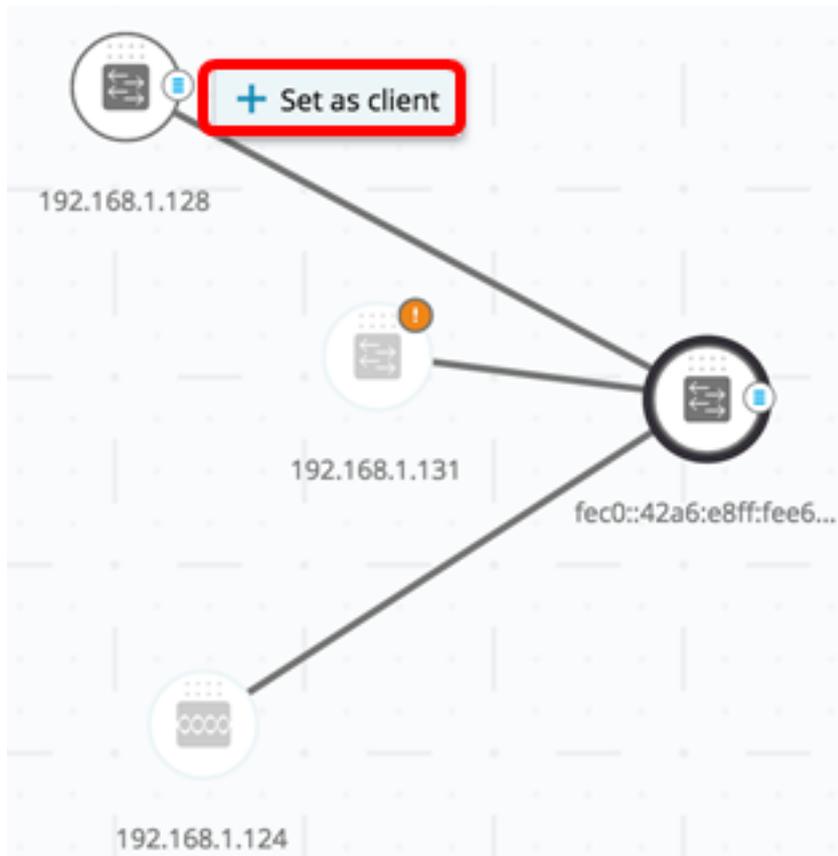


如果交换机已经是DAC RADIUS服务器的客户端，则其IP地址在RADIUS服务器的NAS表中，而RADIUS服务器在其RADIUS服务器表中配置了使用类型802.1X或全部为优先级0。此交换机已预先选择。

如果选择客户端（已为802.1X配置RADIUS服务器，而不是之前选择的服务器），则系统会通知您，程序将中断现有RADIUS服务器操作。

如果选择客户端，该客户端的优先级为0（而不是先前选择的服务器）为802.1X配置了RADIUS服务器，则会显示错误消息，且此客户端上未配置DAC。

步骤6.单击+ Set as client(设置为客户端)。



步骤7.选中客户端交换机端口或端口的复选框以应用802.1X身份验证。

注意：在本示例中，检查GE1/1、GE1/2、GE1/3和GE1/4端口。

< BACK

DONE

Select Client Ports

switche6fa9f / 192.168.1.128

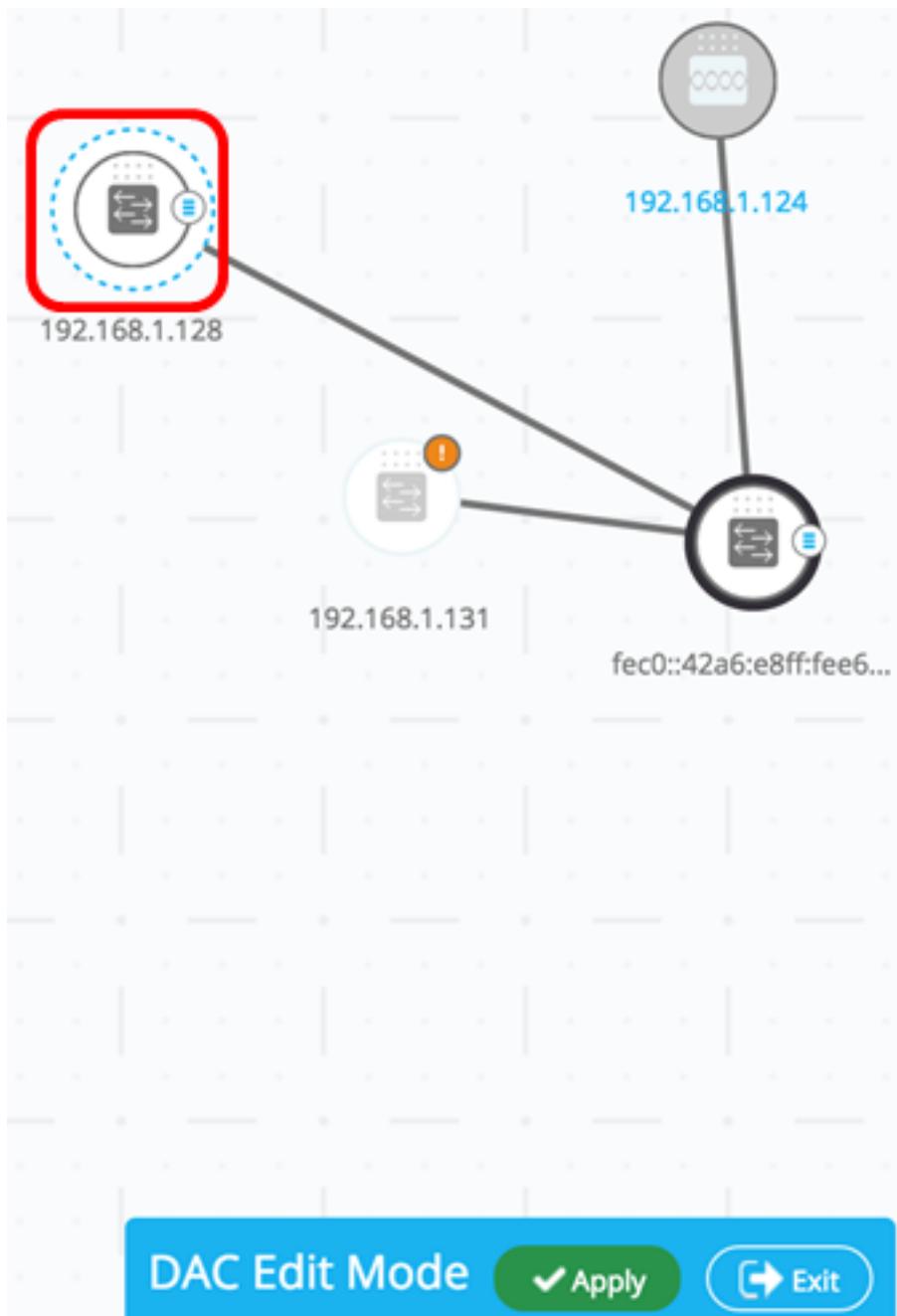
★ Select Recommended

<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		★

注意：SNA建议列出所有边缘端口或未知连接到其他交换机或云的所有端口。

步骤8. (可选) 单击Select Recommended(选择建议)按钮以检查所有推荐端口。

步骤9.单击“完成”。DAC RADIUS客户端在拓扑视图中以虚蓝突出显示。



步骤10.单击“应用”保存更改。

步骤11.输入DAC RADIUS服务器将用于网络上所有客户端的密钥字符串。

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

注意：在本例中，使用Cisco1234。

步骤12. (可选) 将按钮切换为“自动生成”，以使用自动生成的密钥字符串。

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

步骤13.单击页面右上角的继续。

CONTINUE

步骤14.查看更改，然后单击“应用更改”。

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

步骤15. (可选) 如果不想在配置文件中保存设置，请取消选中“保存到启动配置”复选框。

APPLY CHANGES

Save to startup configuration

第16步。(可选) 如果您使用的是只读帐户，系统可能会提示您输入凭据以继续。在“密码”字段中输入密码，然后单击提交。

Upgrade Access Permission ✕



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

Username:

cisco

Password:

SUBMIT

步骤17. Status列应包含绿色复选框，用于确认更改的成功应用。单击“完成”。

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	<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> Add DAC client 192.168.1.128 to server fec0:42a6:...
switche6fa9f 192.168.1.128	Set radius client for 192.168.1.128	<input checked="" type="checkbox"/> DAC configuration for client 192.168.1.128 succeed...

配置DAC后，每当网络上通过启用DAC的RADIUS服务器拒绝新的非阻止列表设备时，系统会显示警报。系统将询问您是将此设备添加到授权设备的允许列表，还是将其发送到阻止列表，以便您不会再次收到警报。

当向用户通知新设备时，SNA提供设备的MAC地址和设备尝试访问网络的端口。

如果从非DAC RADIUS服务器的设备收到拒绝事件，则会忽略该消息，并且会忽略此设备在接下来的20分钟内发出的所有其他消息。20分钟后，SNA再次检查设备是否是DAC RADIUS服务器。如果用户已添加到允许列表，则设备将添加到所有DAC服务器的DAC组。保存此配置后，您可以选择是否立即将此设置保存到服务器的启动配置。默认情况下，此选项处于选中状态。

在设备添加到允许列表之前，不允许其访问网络。只要DAC RADIUS服务器已定义且可访问，您可以随时查看和更改允许和阻止列表。要配置DAC列表管理，请跳至[DAC列表管理](#)。

应用DAC设置时，系统会显示一个报告，其中列出将应用于参与设备的操作。批准更改后，您可以决定是否应将设置额外复制到已配置设备的启动配置文件。最后，应用配置。

如果DAC配置流程的某些步骤丢失，报告将显示警告，以及设备处理的操作状态。

字段	价值	备注
设备	设备标识符（主机名或IP地址）	
操作	DAC服务器可能的操作： <ul style="list-style-type: none"> • 启用RADIUS服务器 • 禁用RADIUS服务器 • 更新客户端列表 • 创建RADIUS服务器组 • 删除RADIUS服务器组 DAC客户端可能执行的操作： <ul style="list-style-type: none"> • 添加RADIUS服务器连接 • 更新RADIUS服务器连接 • 删除RADIUS服务器连接 • 更新802.1x设置 • 更新接口身份验证设置 • 更新接口主机和会话设置 	每台设备可能（而且可能）出现多个操作。 每个操作都可以有自己的状态。
警告	DAC服务器可能出现的警告包括： <ul style="list-style-type: none"> • 所选IP接口是动态的。 DAC客户端可能出现的警告包括： <ul style="list-style-type: none"> • 设备已是不同RADIUS服务器的客户端。 • 未选择端口。 	警告还包含指向DAC部分的链接，这些部分可以在其中处理。 当出现警告时，可以应用更改。
状态	<ul style="list-style-type: none"> • 待处理 • 成功 • 失败 	当状态为故障时，系统会显示操作的错误消息。

DAC列表管理

添加客户端设备并选择其哪些端口要进行身份验证后，这些端口上检测到的所有未身份验证设备都将添加到未身份验证设备列表中。

DAC支持以下设备列表：

- 允许列表 — 包含可进行身份验证的所有客户端的列表。
- 阻止列表 — 包含永远不能进行身份验证的客户端列表。

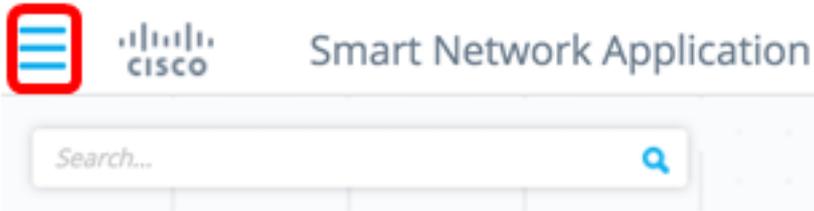
如果要对设备及其端口进行身份验证，则必须将其添加到允许列表。如果不希望对它们进行身份验证，则无需执行任何操作，因为默认情况下，它们将添加到阻止列表。

[有关其他信息，请参阅词汇表。](#)

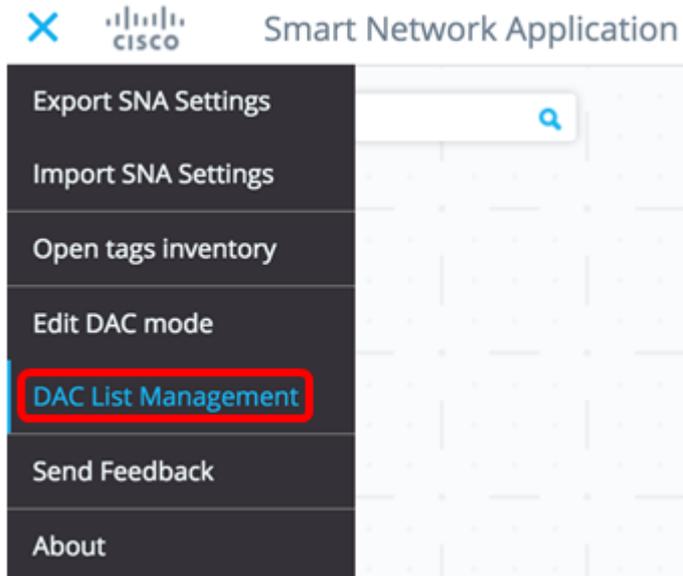
添加要允许的设备列表或阻止列表

要将设备添加到允许列表或阻止列表，请执行以下步骤：

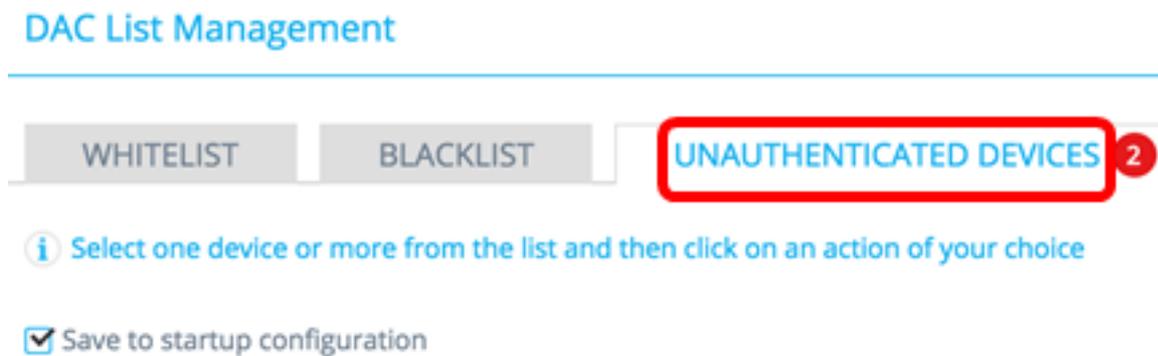
步骤1.单击SNA页左上角的Options菜单以显示可用选项。



步骤2.选择DAC List Management。



步骤3.单击UNAUTHENTICATED DEVICES(未验证设备)选项卡。此页面将显示所有未经身份验证的设备的列表。



注意：或者，您也可以点击SNA页面右上角的DAC列表管理系统图标。



步骤4. (可选) 选中要添加到允许列表的设备或设备的MAC地址旁的复选框，然后点击添加到允许列表。

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

步骤5. (可选) 选中要添加到阻止列表的设备或设备的MAC地址旁的复选框，然后点击添加到阻止列表(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

步骤6. (可选) 选中要关闭的设备或设备的MAC地址旁的复选框，然后单击Dismiss。

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

<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

注意：在设备端口上输入的所有数据包都在RADIUS服务器上身份验证。

现在，您应该已将设备添加到“允许”列表或“阻止”列表。

管理允许列表或阻止列表上的设备

要管理允许或阻止列表，请相应地单击“允许列表”或“阻止列表”。

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	
--------------------------	-------------------	--

您可以在这些页面中执行以下任务：

- 从列表中删除 — 此操作从列表中删除所选设备。
- 移动到阻止列表或移动到允许列表 — 此操作将所选设备移到指定列表。
- 添加设备 — 此操作通过输入设备的MAC地址并单击“添加+”按钮，将设备添加到阻止或允许列表中。

- 使用MAC地址搜索设备 — 输入MAC地址，然后点击 **搜索**  按钮。

您现在应该已管理DAC列表上的设备。