

スマートネットワークアプリケーション(SNA)によるデバイス承認制御(DAC)管理の設定

目的

スマートネットワークアプリケーション(SNA)システムは、デバイスとトラフィックの詳細なモニタリング情報を含むネットワークトポロジの概要を表示します。SNAを使用すると、ネットワーク内でサポートされているすべてのデバイス上の設定をグローバルに表示および変更できます。

SNAには、デバイス認証制御(DAC)と呼ばれる機能があり、ネットワーク内の許可されたクライアントデバイスのリストを設定できます。DACはネットワーク内のSNAデバイス上で802.1X機能をアクティブ化し、組み込みのリモート認証ダイヤルインユーザサービス(RADIUS)またはRADIUSホストサーバは、いずれかのSNAデバイス上で設定できます。DACはMedia Access Control(MAC)認証を介して実行されます。

この記事では、SNAを使用してDAC管理を設定する方法について説明します。

該当するデバイス

- Sx350シリーズ
- SG350Xシリーズ
- Sx550Xシリーズ

注：Sx250シリーズのデバイスは、ネットワークに接続するとSNA情報を提供できますが、これらのデバイスからSNAを起動することはできません。

[Software Version]

- 2.2.5.68

DACワークフロー

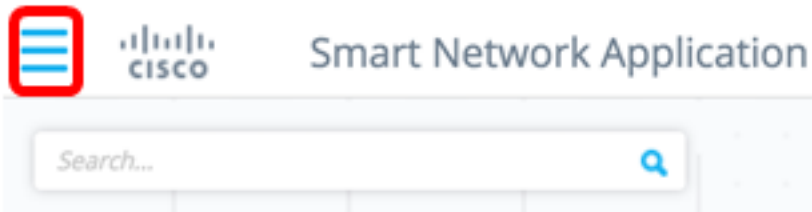
DAC管理は、次の手順で設定できます。

- [DACの有効化](#)
- [RADIUSサーバとクライアントの設定](#)
- [DACリスト管理](#)

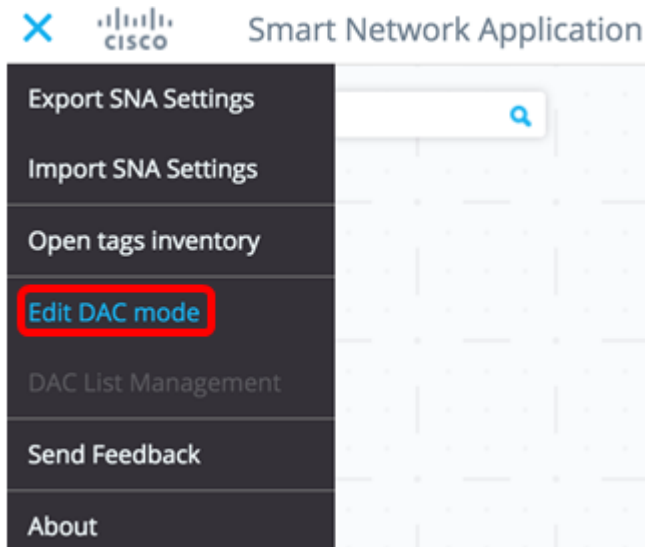
[DACの有効化](#)

DACにアクセスしてアクティブにするには、次の手順を実行します。

ステップ1:SNAページの左上の[オプション]メニューをクリックして、使用可能なオプションを表示します。



ステップ2:[Edit DAC mode]を選択します。



DAC編集モードがアクティブになりました。トポロジマップの下に青いフレームが表示され、画面下部にコントロールパネルが表示されます。



ステップ3: (オプション) DAC編集モードを終了するには、[終了]ボタンをクリックします。

RADIUSサーバとクライアントの設定

ステップ1:[Topology]ビューで、SNAデバイスのいずれかを選択し、[Options]メニューをクリックします。



ステップ2:[+ Set as DAC server]をクリックします。



ステップ3: デバイスに複数のIPアドレスがある場合は、それらのアドレスのいずれかをDACで使用するアドレスとして選択します。この例では、192.168.1.127です |静的が選択されています。

< 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

注：アドレスのリストは、IPインターフェイスがスタティックかダイナミックかを示します。ダイナミックIPを選択すると、接続が不安定になる可能性があることに注意してください。

Select IP Address

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

IP ADDRESS

192.168.1.127 | Dynamic

⚠ Dynamic ip might cause an unstable connection

DONE

ステップ4:[完了]をクリックします。

< BACK

Select IP Address

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

IP ADDRESS

DONE

注：既存のDACサーバを編集する場合、そのクライアントによって現在使用されているアドレスが事前に選択されます。

DAC RADIUSサーバは、[Topology]ビューでソリッドで強調表示されます。



ステップ5:SNAデバイスの1つを選択し、[Options]メニューをクリックします。

注：クライアントが選択されていない場合は、設定を適用できません。

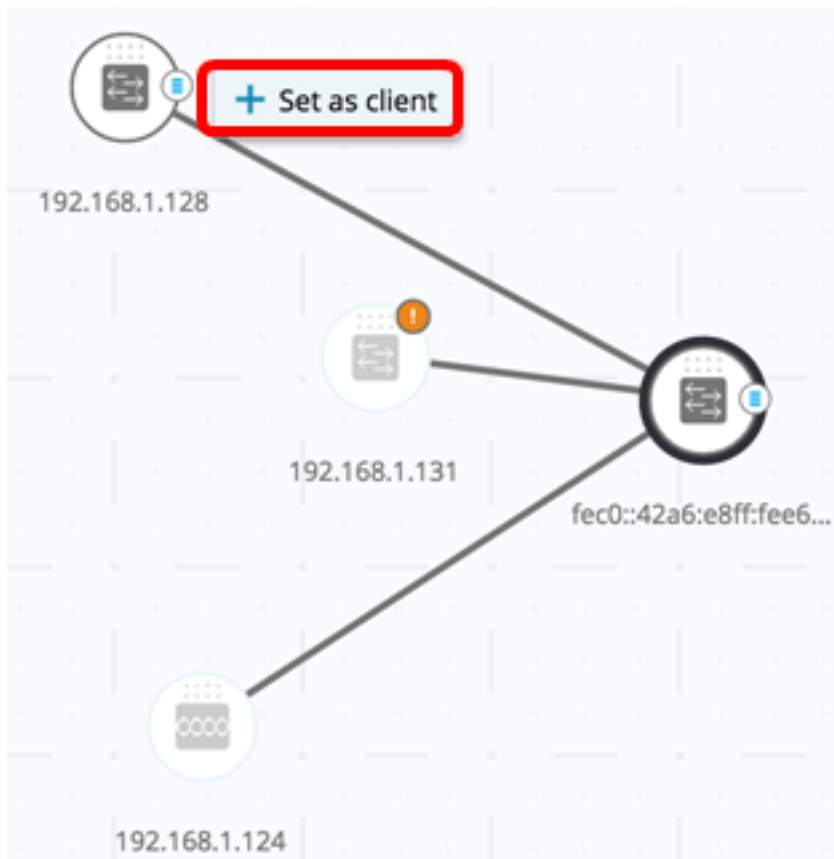


スイッチが既にDAC RADIUSサーバのクライアントである場合、そのIPアドレスはRADIUSサーバのNASテーブルにあり、RADIUSサーバは使用タイプ802.1Xまたはすべてプライオリティ0でRADIUSサーバテーブルに設定されます。

すでに802.1X用に設定されているRADIUSサーバが先に選択したサーバ以外のクライアントを選択すると、既存のRADIUSサーバの動作が中断されることが通知されます。

以前に選択したサーバ以外の優先度0で802.1Xに設定されたRADIUSサーバを持つクライアントを選択すると、エラーメッセージが表示され、DACはこのクライアントで設定されません。

ステップ6:[+ Set as client]をクリックします。



ステップ7:802.1X認証を適用するには、クライアントスイッチのポートのチェックボックスまたはチェックボックスをオンにします。

注：この例では、GE1/1、GE1/2、GE1/3、およびGE1/4ポートがチェックされています。

< BACK

DONE

Select Client Ports

switche6fa9f / 192.168.1.128

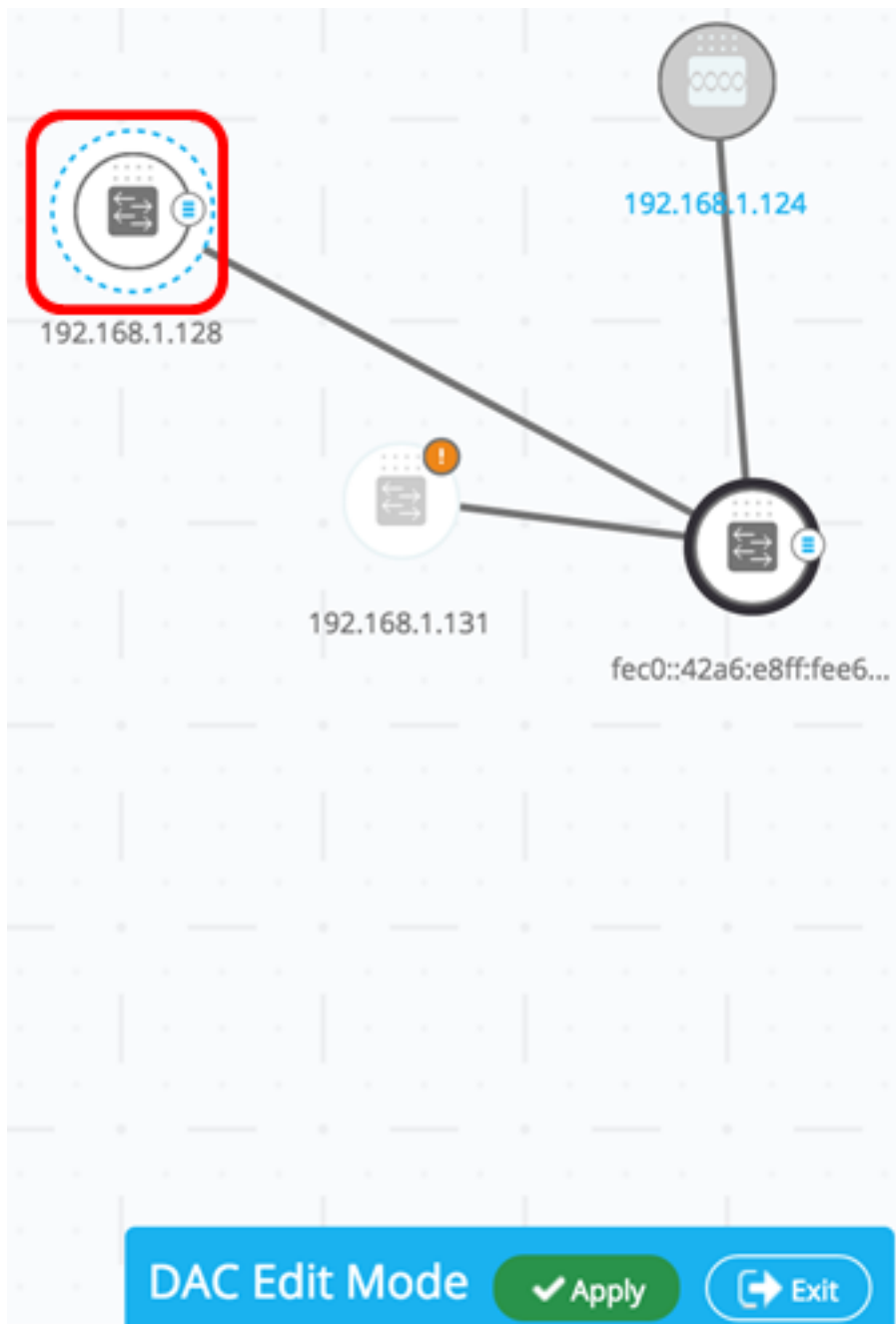
★ Select Recommended

<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：SNAでは、すべてのエッジポート、または他のスイッチやクラウドに接続されていないすべてのポートのリストを推奨しています。

ステップ8: (オプション) すべての推奨ポートを確認するには、[Select Recommended]ボタンをクリックします。

ステップ9:[完了]をクリックします。DAC RADIUSクライアントは、[Topology]ビューで青色の破線で強調表示されます。



ステップ10:[Apply]をクリックして、変更を保存します。

ステップ11：ネットワーク上のすべてのクライアントでDAC RADIUSサーバが使用するキーリングを入力します。

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：この例では、Cisco1234が使用されています。

ステップ12: (オプション) 自動生成されたキースtringを使用するには、ボタンを[自動生成]に切り替えます。

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

ステップ13 : ページの右上隅にある[Continue]をクリックします。

CONTINUE

ステップ14 : 変更を確認し、[APPLY CHANGES]をクリックします。

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

ステップ15: (オプション) 設定ファイルに設定を保存しない場合は、[スタートアップコンフィギュレーションに保存]チェックボックスをオフにします。

APPLY CHANGES

Save to startup configuration

ステップ16: (オプション) 読み取り専用アカウントを使用している場合は、続行するために資格情報の入力を求められます。[パスワード]フィールドにパスワードを入力し、[送信]をクリックします。

Upgrade Access Permission ×



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

Username:

cisco

Password:

SUBMIT

ステップ17:[Status (ステータス)]列に、変更の適用が成功したことを確認する緑色のチェックボックスが表示されます。[Done] をクリックします。

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 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...

DACの設定後、DAC対応RADIUSサーバを介してネットワーク上の新しい非ブロックリストのデバイスが拒否されるたびにアラートが表示されます。このデバイスを承認されたデバイスの許可リストに追加するか、ブロックのリストに送信して再び警告を受けないようにするかを尋ねられます。

新しいデバイスをユーザに通知すると、SNAはデバイスのMACアドレスと、デバイスがネットワークにアクセスしようとしたポートを提供します。

DAC RADIUSサーバ以外のデバイスから拒否イベントが受信された場合、メッセージは無視され、このデバイスからの今後の20分間のメッセージはすべて無視されます。20分後、SNAはデバイスがDAC RADIUSサーバであるかどうかを再度確認します。ユーザが許可リストに追加されると、デバイスはすべてのDACサーバのDACグループに追加されます。この設定を保存すると、この設定をサーバのスタートアップコンフィギュレーションに即座に保存するかどうかを選択できます。このオプションはデフォルトで選択されています。

デバイスが許可リストに追加されるまで、ネットワークへのアクセスは許可されません。

DAC RADIUSサーバが定義され、到達可能である限り、許可リストとブロックリストはいつでも表示および変更できます。DACリスト管理を構成するには、DACリスト管理に[進んでください](#)。

DAC設定を適用すると、参加デバイスに適用されるアクションを示すレポートが表示されます。変更を承認したら、設定を設定済みデバイスのスタートアップコンフィギュレーションファイルに追加でコピーするかどうかを決定できます。最後に、設定を適用します。

このレポートには、DAC設定プロセスの一部のステップが失われた場合に、デバイスが処理したアクションのステータスとともに警告が表示されます。

	注
<p>デバイスID (ホスト名またはIPアドレス)</p>	
<p>サーバーで可能な操作 :</p> <ul style="list-style-type: none"> DACサーバの有効化 DACサーバの無効化 クライアントリストの更新 DACサーバグループの作成 DACサーバグループの削除 <p>クライアントで可能なアクション :</p> <ul style="list-style-type: none"> DACサーバ接続の追加 DACサーバ接続の更新 DACサーバ接続の削除 2.1x設定の更新 インターフェイス認証設定の更新 インターフェイスホストとセッション設定の更新 	<p>各デバイスに対して複数のアクションが表示される可能性があります。各アクションには独自のステータスがあります。</p>
<p>DACサーバに関する警告には、次のものがあります。</p> <ul style="list-style-type: none"> 選択したIPインターフェイスはダイナミックです。 クライアントに関する警告には、次のものがあります。 <p>デバイスはすでに別のRADIUSサーバのクライアントでポートが選択されていません。</p>	<p>警告には、対処できるDACのセクションへのリンクも変更は、警告が存在する場合に適用できます。</p>
<p>pending</p> <p>成功</p> <p>失敗</p>	<p>ステータスが障害の場合、アクションのエラーメッセージです。</p>

[DACリスト管理](#)

クライアントデバイスを追加し、どのポートを認証するかを選択すると、それらのポートで検出されたすべての非認証デバイスが非認証デバイスのリストに追加されます。

DACは、次のデバイスのリストをサポートしています。

- [Allow List] : 認証可能なすべてのクライアントのリストが含まれます。
- Block List : 認証を受けないクライアントのリストが含まれます。

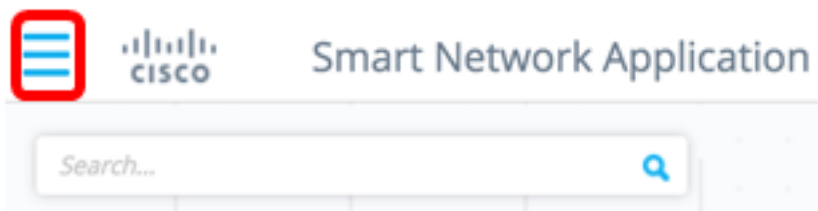
デバイスとそのポートを認証するには、許可リストに追加する必要があります。これらのユーザを認証したくない場合は、デフォルトでブロックリストに追加されるため、アクションは必要ありません。

[詳細については、用語集を参照してください。](#)

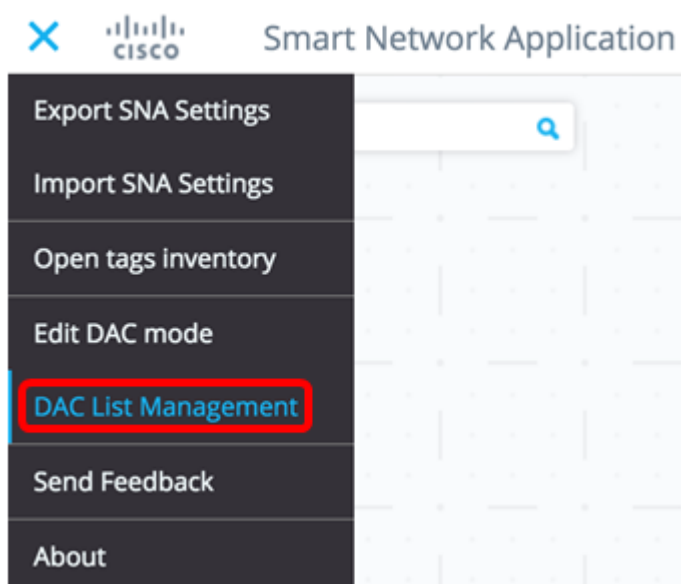
許可リストまたはブロックリストへのデバイスの追加

許可リストまたはブロックリストにデバイスを追加するには、次の手順を実行します。

ステップ1:SNAページの左上の[オプション]メニューをクリックして、使用可能なオプションを表示します。



ステップ2:[DAC List Management]を選択します。



ステップ3:[UNAUTHENTICATED DEVICES]タブをクリックします。このページには、すべての非認証デバイスのリストが表示されます。

DAC List Management



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

Save to startup configuration

注：または、SNAページの右上隅にある[DAC List Management System]アイコンをクリックすることもできます。

ステップ4: (オプション) 許可リストに追加するデバイスのMACアドレスの横にあるチェックボックスをオンにし、[許可リストに追加(Add to Allow list)]をクリックします。

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

ステップ5: (オプション) ブロックリストに追加する1つ以上のデバイスのMACアドレスの横にあるチェックボックスをオンにし、[ブロックリストに追加]をクリックします。

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

ステップ6: (オプション) 終了するデバイスのMACアドレスの横にあるチェックボックスをオンにし、[Dismiss]をクリックします。

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

注：デバイスのポートに入るすべてのパケットは、RADIUSサーバで認証されます。

これで、許可リストまたはブロックリストにデバイスが追加されました。

許可リストまたはブロックリストでのデバイスの管理

許可リストまたはブロックリストを管理するには、「許可リスト」(ALLOW LIST)タブまたは「ブロックリスト」(BLOCK LIST)タブを適宜選択します。

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

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

これらのページでは、次のタスクを実行できます。

- [リストから削除(Remove from list)]：選択した1つ以上のデバイスをリストから削除します。
- [ブロックリストに移動(Move to Block list)]または[許可リストに移動(Move to Allow list)]：このアクションは、選択した1つまたは複数のデバイスを指定したリストに移動します。

- デバイスの追加：このアクションは、MACアドレスを入力し、[ADD +]ボタンをクリックして、ブロックまたは許可リストのいずれかにデバイスを追加します。
- MACアドレスを使用したデバイスの検索：MACアドレスを入力し、検索  をクリックして、クエリーを実行します。

これで、DACリストのデバイスを管理できました。