

Konfigurieren des DAC-Managements (Device Authorization Control) über eine Smart Network Application (SNA)

Ziel

Das SNA-System (Smart Network Application) bietet einen Überblick über die Netzwerktopologie mit detaillierten Überwachungsinformationen für Geräte und Datenverkehr. SNA ermöglicht das globale Anzeigen und Ändern von Konfigurationen auf allen unterstützten Geräten im Netzwerk.

SNA verfügt über eine Funktion, die als Device Authorization Control (DAC) bezeichnet wird und mit der Sie eine Liste der autorisierten Client-Geräte im Netzwerk konfigurieren können. DAC aktiviert 802.1X-Funktionen auf SNA-Geräten im Netzwerk. Auf einem der SNA-Geräte kann ein integrierter Remote Authentication Dial-In User Service (RADIUS) oder RADIUS Host Server konfiguriert werden. DAC wird mittels MAC-Authentifizierung (Media Access Control) durchgeführt.

Dieser Artikel enthält Anweisungen zur Konfiguration der DAC-Verwaltung über SNA.

Anwendbare Geräte

- Serie Sx350
- SG350X-Serie
- Serie Sx550X

Hinweis: Geräte der Serie Sx250 können SNA-Informationen bereitstellen, wenn sie mit dem Netzwerk verbunden sind. SNA kann jedoch nicht von diesen Geräten aus gestartet werden.

Softwareversion

- 2,2 5,68

DAC-Workflow

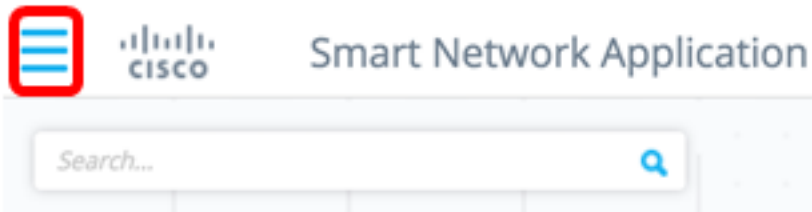
Sie können die DAC-Verwaltung wie folgt konfigurieren:

- [DAC aktivieren](#)
- [Konfigurieren von RADIUS-Servern und -Clients](#)
- [DAC-Listenverwaltung](#)

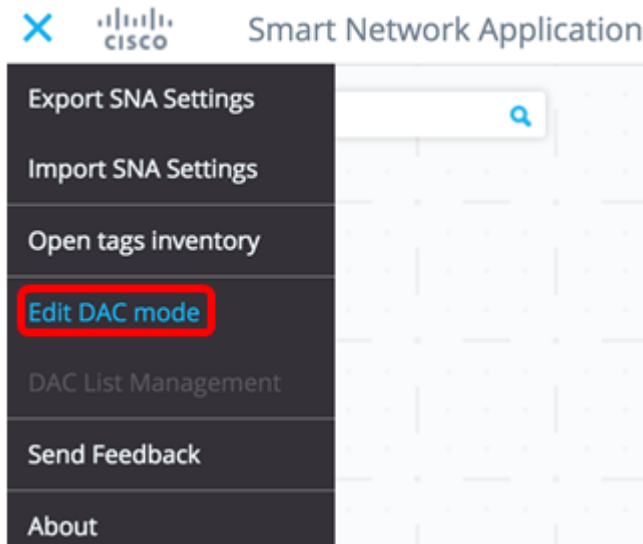
[DAC aktivieren](#)

Um auf das DAC zuzugreifen und es zu aktivieren, gehen Sie wie folgt vor:

Schritt 1: Klicken Sie auf das Menü **Optionen** in der linken oberen Ecke der SNA-Seite, um die verfügbaren Optionen anzuzeigen.



Schritt 2: Wählen Sie **DAC-Modus bearbeiten** aus.



Der DAC-Bearbeitungsmodus ist jetzt aktiviert. Sie sollten den blauen Rahmen unter der Topologieübersicht und das Bedienfeld am unteren Bildschirmrand sehen.



Schritt 3: (Optional) Um den DAC-Bearbeitungsmodus zu beenden, klicken Sie auf die Schaltfläche **Beenden**.

Konfigurieren von RADIUS-Servern und -Clients

Schritt 1: Wählen Sie in der Topologieansicht eines der SNA-Geräte aus, und klicken Sie auf das entsprechende Menü **Optionen**.



Schritt 2: Klicken Sie auf **+ Als DAC-Server festlegen**.



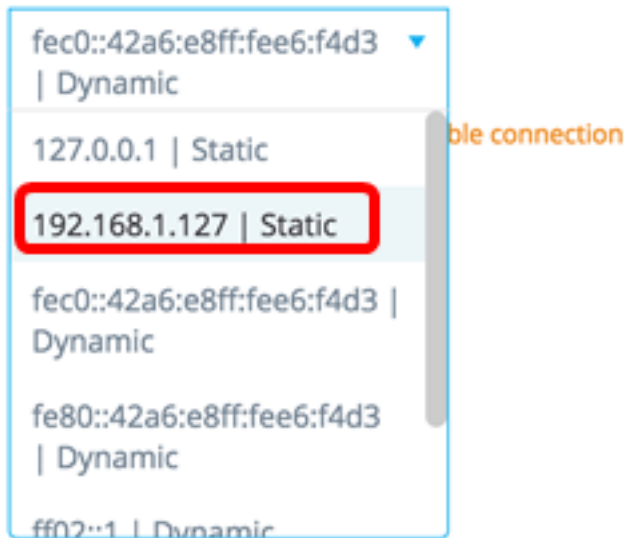
Schritt 3: Wenn das Gerät mehr als eine IP-Adresse hat, wählen Sie eine dieser Adressen als die von DAC zu verwendende Adresse aus. In diesem Beispiel wird 192.168.1.127 | Statisch ausgewählt.

< BACK

Select IP Address

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

IP ADDRESS




A screenshot of a mobile application's IP address selection menu. The menu is a list with a scroll bar on the right. The first item is 'fec0::42a6:e8ff:fee6:f4d3 | Dynamic'. The second item is '127.0.0.1 | Static'. The third item, '192.168.1.127 | Static', is highlighted with a red rectangular border. The fourth item is 'fec0::42a6:e8ff:fee6:f4d3 | Dynamic'. The fifth item is 'fe80::42a6:e8ff:fee6:f4d3 | Dynamic'. The sixth item is 'ff02::1 | Dynamic'. An orange arrow points to the right side of the menu with the text 'Unstable connection'.

Hinweis: Die Liste der Adressen gibt an, ob die IP-Schnittstelle statisch oder dynamisch ist. Sie werden gewarnt, dass die Auswahl einer dynamischen IP-Adresse zu einer instabilen Verbindung führen kann.

Select IP Address

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

IP ADDRESS



A screenshot of the same mobile application's IP address selection menu. The menu is now a single dropdown box. The selected item is '192.168.1.127 | Dynamic'.

⚠ Dynamic ip might cause an unstable connection

DONE

Schritt 4: Klicken Sie auf **Fertig**.

< BACK

Select IP Address

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

IP ADDRESS

192.168.1.127 |
Static

DONE

Hinweis: Beim Bearbeiten eines vorhandenen DAC-Servers wird die aktuell von den Clients verwendete Adresse vorausgewählt.

Der DAC RADIUS-Server wird in der Topologieansicht durchgehend hervorgehoben.



Schritt 5: Wählen Sie eines der SNA-Geräte aus, und klicken Sie auf das Menü Optionen.

Hinweis: Wenn keine Clients ausgewählt sind, können Sie die Einstellungen nicht übernehmen.

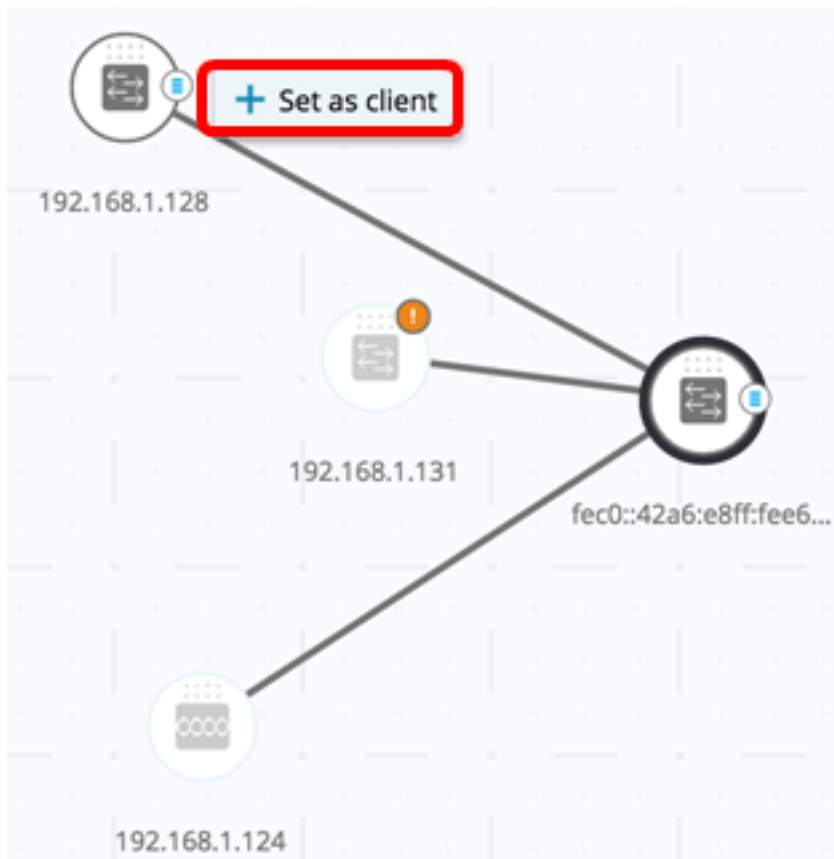


Wenn ein Switch bereits ein Client des DAC RADIUS-Servers ist, befindet sich seine IP-Adresse in der NAS-Tabelle des RADIUS-Servers, und der RADIUS-Server ist in seiner RADIUS-Servertabelle mit dem Auslastungstyp 802.1X oder mit der Priorität 0 konfiguriert. Dieser Switch ist vorausgewählt.

Wenn ein Client ausgewählt ist, für den bereits ein RADIUS-Server für 802.1X konfiguriert ist, der nicht der zuvor ausgewählte Server ist, werden Sie darüber informiert, dass der Vorgang den vorhandenen RADIUS-Serverbetrieb unterbricht.

Wenn ein Client ausgewählt wird, auf dem ein RADIUS-Server für 802.1X mit der Priorität 0 konfiguriert ist, der nicht der zuvor ausgewählte Server ist, wird eine Fehlermeldung angezeigt, und auf diesem Client wird kein DAC konfiguriert.

Schritt 6: Klicken Sie auf **+ Als Client festlegen**.



Schritt 7: Aktivieren Sie das Kontrollkästchen oder Kontrollkästchen des Ports oder der Ports des Client-Switches, um 802.1X-Authentifizierungen anzuwenden.

Hinweis: In diesem Beispiel werden GE1/1-, GE1/2-, GE1/3- und GE1/4-Ports überprüft.

< BACK

DONE

Select Client Ports

switche6fa9f / 192.168.1.128

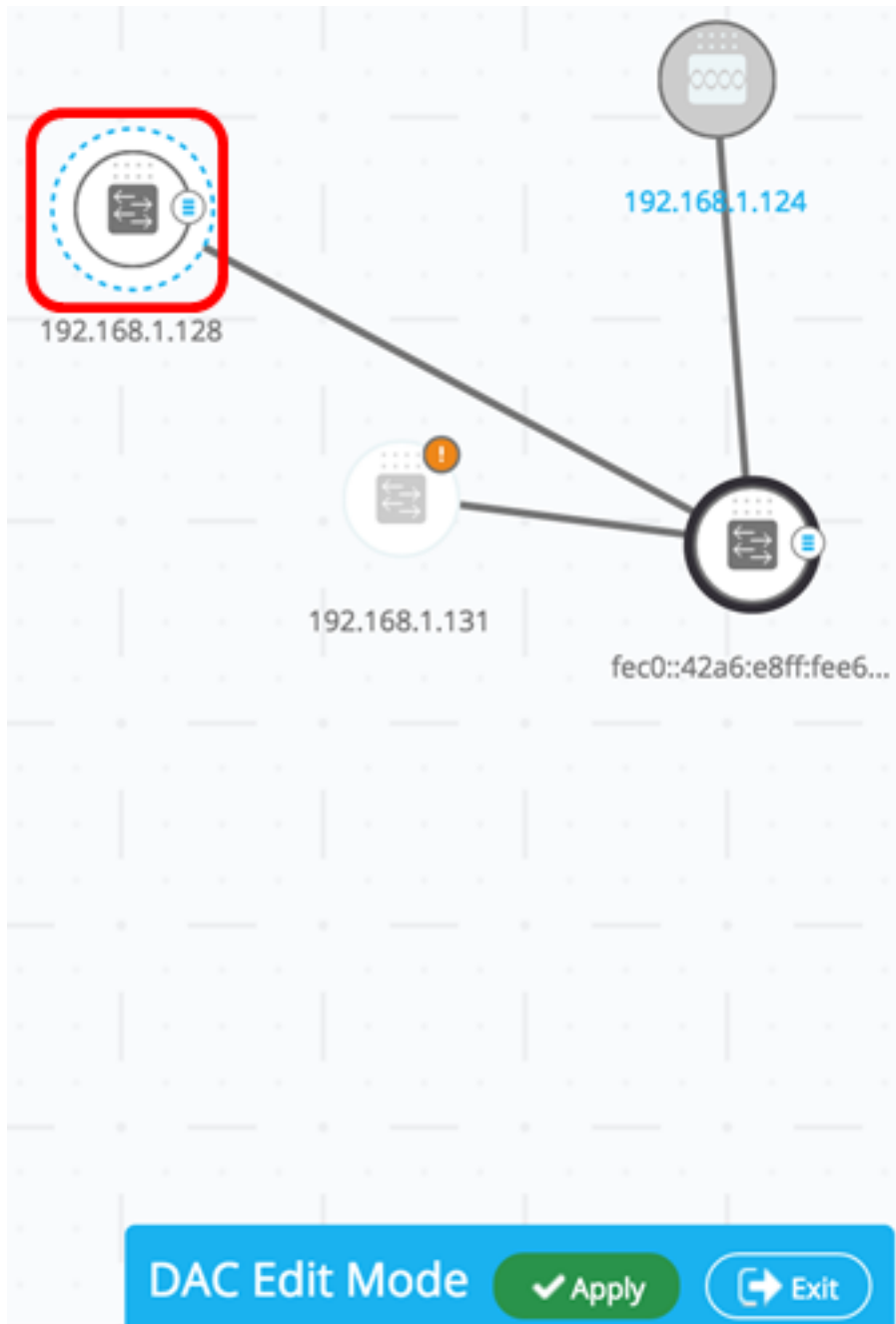
★ Select Recommended

| <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 | | ★ |

Hinweis: Die SNA empfiehlt eine Liste aller Edge-Ports oder aller Ports, die nicht mit anderen Switches oder Clouds verbunden sind.

Schritt 8: (Optional) Klicken Sie auf die Schaltfläche **Select Recommended** (Empfohlen auswählen), um alle empfohlenen Ports zu überprüfen.

Schritt 9: Klicken Sie auf **Fertig**. Der DAC RADIUS-Client wird in der Topologieansicht in gestricheltem Blau hervorgehoben.



Schritt 10: Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Schritt 11: Geben Sie einen Keystring ein, der vom DAC RADIUS-Server mit allen Clients im Netzwerk verwendet wird.

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

Hinweis: In diesem Beispiel wird Cisco1234 verwendet.

Schritt 12: (Optional) Schalten Sie die Schaltfläche auf **Automatisch generiert um**, um einen automatisch generierten Keystring zu verwenden.

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

Schritt 13: Klicken Sie in der rechten oberen Ecke der Seite auf **Weiter**.

CONTINUE

Schritt 14: Überprüfen Sie die Änderungen, und klicken Sie dann auf **ÄNDERUNGEN ANWENDEN**.

Apply ×

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

Save to startup configuration

| SWITCH | ACTIONS |
|--|--|
| switche6f4d3 fec0:42a6ce8ff:fee6cf4d3 | Set radius server fec0:42a6ce8ff:fee6cf4d3 |
| switche6fa9f 192.168.1.128 | Add radius client 192.168.1.128 to server fec0:42a6ce8ff:fee6cf4d3 |
| switche6fa9f 192.168.1.128 | Set radius client for 192.168.1.128 |

Schritt 15: (Optional) Deaktivieren Sie das Kontrollkästchen **In Startkonfiguration speichern**, wenn Sie die Einstellungen in der Konfigurationsdatei nicht speichern möchten.

APPLY CHANGES

Save to startup configuration

Schritt 16: (Optional) Wenn Sie ein schreibgeschütztes Konto verwenden, werden Sie möglicherweise aufgefordert, Ihre Anmeldeinformationen einzugeben, um fortzufahren. Geben Sie das Kennwort in das Feld *Kennwort ein*, und klicken Sie dann auf **SENDEN**.

Upgrade Access Permission ✕



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

Username:

cisco

Password:

SUBMIT

Schritt 17: Die Spalte Status sollte grüne Kontrollkästchen enthalten, die die erfolgreiche Anwendung der Änderungen bestätigen. Klicken Sie auf **Fertig**.

Apply

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

DONE

Save to startup configuration

| SWITCH | ACTIONS | STATUS |
|--|---|---|
| switche664d3 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... |

Nach der Konfiguration des DAC wird immer dann eine Warnmeldung angezeigt, wenn ein neues, nicht in der Sperrliste enthaltenes Gerät über einen RADIUS-Server mit DAC-Unterstützung im Netzwerk abgelehnt wird. Sie werden gefragt, ob Sie dieses Gerät der Zulassungsliste der autorisierten Geräte hinzufügen oder es in eine Sperrliste senden möchten, damit Sie nicht erneut benachrichtigt werden.

Wenn der Benutzer über das neue Gerät informiert wird, stellt SNA die MAC-Adresse des Geräts und den Port bereit, auf den das Gerät versucht hat, auf das Netzwerk zuzugreifen.

Wenn ein Ablehnungsereignis von einem Gerät empfangen wird, das kein DAC RADIUS-Server ist, wird die Meldung ignoriert, und alle weiteren Meldungen dieses Geräts für die nächsten 20 Minuten werden ignoriert. Nach 20 Minuten überprüft SNA erneut, ob es sich bei dem Gerät um einen DAC RADIUS-Server handelt. Wenn ein Benutzer der Zulassungsliste hinzugefügt wird, wird das Gerät der DAC-Gruppe aller DAC-Server hinzugefügt. Wenn diese Konfiguration gespeichert wird, können Sie festlegen, ob diese Einstellung sofort in der Startkonfiguration des Servers gespeichert werden soll. Diese

Option ist standardmäßig ausgewählt.

Bis ein Gerät der Zulassungsliste hinzugefügt wird, ist der Zugriff auf das Netzwerk nicht zulässig. Sie können die Zulassen- und Blocklisten jederzeit anzeigen und ändern, solange ein RADIUS-Server des DAC definiert und erreichbar ist. Zum Konfigurieren der DAC-Listenverwaltung fahren Sie mit [DAC List Management fort](#).

Beim Anwenden der DAC-Einstellungen wird Ihnen ein Bericht mit Aktionen angezeigt, die auf die teilnehmenden Geräte angewendet werden. Nachdem Sie die Änderungen genehmigt haben, können Sie entscheiden, ob die Einstellungen zusätzlich in die Startkonfigurationsdatei der konfigurierten Geräte kopiert werden sollen. Wenden Sie schließlich die Konfigurationen an.

Der Bericht zeigt Warnungen, wenn einige Schritte des DAC-Konfigurationsprozesses verpasst wurden, sowie den Status der Aktionen, die von den Geräten verarbeitet wurden.

| Feld | Wert | Kommentare |
|-----------|--|--|
| Gerät | Die Geräte-IDs (Hostname oder IP-Adresse) | |
| Aktion | <p>Mögliche Aktionen für den DAC-Server:</p> <ul style="list-style-type: none"> • RADIUS-Server aktivieren • RADIUS-Server deaktivieren • Clientliste aktualisieren • RADIUS-Servergruppe erstellen • RADIUS-Servergruppe löschen <p>Mögliche Aktionen für den DAC-Client:</p> <ul style="list-style-type: none"> • RADIUS-Serververbindung hinzufügen • RADIUS-Serververbindung aktualisieren • Entfernen der RADIUS-Serververbindung • 802.1x-Einstellungen aktualisieren • Einstellungen für die Schnittstellenauthentifizierung aktualisieren • Aktualisieren der Host- und Sitzungseinstellungen der Schnittstelle | <p>Es ist möglich (und wahrscheinlich), dass für jedes Gerät mehrere Aktionen angezeigt werden. Jede Aktion kann ihren eigenen Status haben.</p> |
| Warnungen | Zu den möglichen Warnungen für den DAC- | Warnungen enthalten auch |

| | | |
|--------|---|--|
| | <p>Server gehören:</p> <ul style="list-style-type: none"> • Die ausgewählte IP-Schnittstelle ist dynamisch. <p>Zu den möglichen Warnungen für DAC-Clients gehören:</p> <ul style="list-style-type: none"> • Das Gerät ist bereits ein Client eines anderen RADIUS-Servers. • Es sind keine Ports ausgewählt. | <p>Links zu den Abschnitten des DAC, in denen sie behandelt werden können. Änderungen können angewendet werden, wenn Warnungen vorhanden sind.</p> |
| Status | <ul style="list-style-type: none"> • Ausstehend • Erfolg • Fehler | <p>Wenn der Status ein Fehler ist, wird die Fehlermeldung für die Aktion angezeigt.</p> |

DAC-Listenverwaltung

Wenn Sie Clientgeräte hinzugefügt und ausgewählt haben, welche Ports authentifiziert werden sollen, werden alle auf diesen Ports erkannten nicht authentifizierten Geräte der Liste der nicht authentifizierten Geräte hinzugefügt.

DAC unterstützt die folgenden Gerätelisten:

- Zulassungsliste - Enthält die Liste aller Clients, die authentifiziert werden können.
- Sperrliste - **Enthält** die Liste der Clients, die nie authentifiziert werden dürfen.

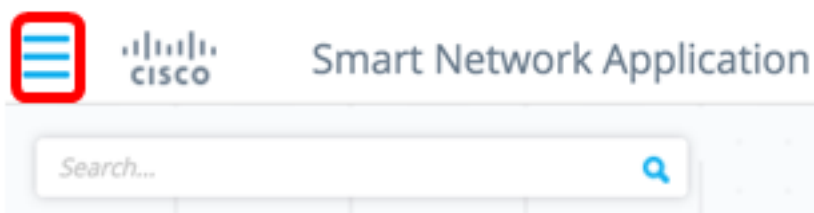
Wenn Geräte und ihre Ports authentifiziert werden sollen, müssen sie den Zulassungslisten hinzugefügt werden. Wenn sie nicht authentifiziert werden sollen, ist keine Aktion erforderlich, da sie standardmäßig der Blockliste hinzugefügt werden.

[Weitere Informationen finden Sie im Glossar.](#)

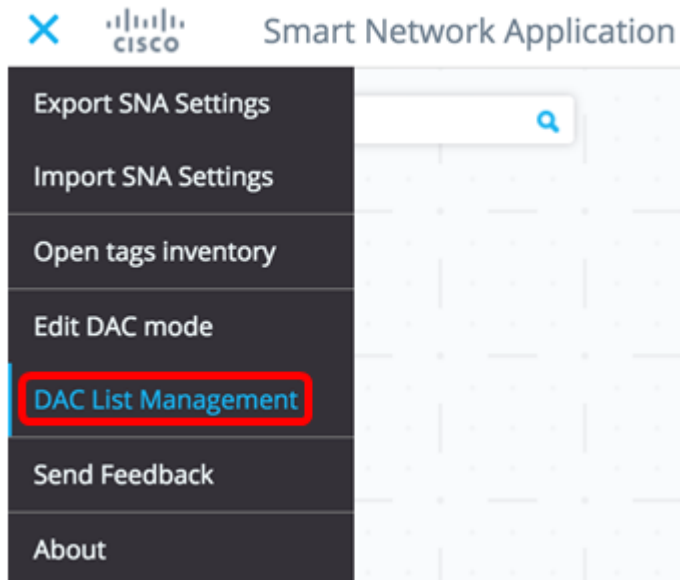
Hinzufügen von Geräten zur Liste Zulassen oder Sperrliste

So fügen Sie Geräte zur Zulassungsliste oder Sperrliste hinzu:

Schritt 1: Klicken Sie auf das Menü **Optionen** in der linken oberen Ecke der SNA-Seite, um die verfügbaren Optionen anzuzeigen.

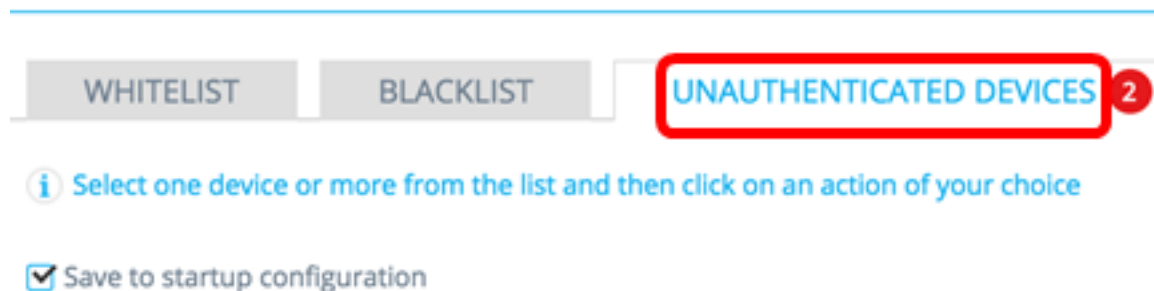


Schritt 2: Wählen Sie **DAC List Management** aus.



Schritt 3: Klicken Sie auf die Registerkarte **UNAUTHENTIFIZIERTE GERÄTE**. Auf dieser Seite wird die Liste aller nicht authentifizierten Geräte angezeigt.

DAC List Management



Hinweis: Sie können auch auf das Symbol DAC List Management System (DAC-Listenverwaltungssystem) in der rechten oberen Ecke der SNA-Seite klicken.



Schritt 4: (Optional) Aktivieren Sie das Kontrollkästchen neben der MAC-Adresse des Geräts (der Geräte), das (die) Sie der Zulassungsliste hinzufügen möchten, und klicken Sie auf **Zu Zulassungsliste hinzufügen**.

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 |

Schritt 5: (Optional) Aktivieren Sie das Kontrollkästchen neben der MAC-Adresse des Geräts oder der Geräte, das bzw. die Sie der Sperrliste hinzufügen möchten, und klicken Sie auf **Zu Sperrliste hinzufügen**.

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 |

Schritt 6: (Optional) Aktivieren Sie das Kontrollkästchen neben der MAC-Adresse des Geräts bzw. der Geräte, das bzw. die Sie entfernen möchten, und klicken Sie auf **"Ablehnen"**.

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 |

Hinweis: Alle Pakete, die auf den Ports des Geräts eingehen, werden auf dem RADIUS-Server authentifiziert.

Sie sollten jetzt ein Gerät zur Zulassungsliste oder Sperrliste hinzugefügt haben.

Verwalten von Geräten in der Liste Zulassen oder Sperrliste

Zum Verwalten der Zulassen- oder Blocklisten klicken Sie auf die Registerkarte **LIST ZULASSEN** oder **BLOCKLISTE**.

DAC List Management

WHITELIST **BLACKLIST** UNAUTHENTICATED DEVICES

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 Enter MAC Address **ADD +**

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

Auf diesen Seiten können Sie die folgenden Aufgaben ausführen:

- Aus Liste entfernen: Mit dieser Aktion werden die ausgewählten Geräte aus der Liste entfernt.
- Zur Sperrliste verschieben oder In Zulassungsliste verschieben: Mit dieser Aktion werden die

ausgewählten Geräte in die angegebene Liste verschoben.

- Gerät hinzufügen: Mit dieser Aktion wird dem Block oder der Zulassungsliste ein Gerät hinzugefügt, indem die MAC-Adresse eingegeben und die **ADD+**-Schaltfläche angeklickt wird.
- Suchen Sie ein Gerät mithilfe der MAC-Adresse. Geben Sie eine MAC-Adresse ein, und klicken Sie auf **Suchen**  -Taste.

Sie sollten jetzt die Geräte in der DAC-Liste verwalten.