Configurer la gestion du contrôle d'autorisation de périphérique (DAC) via Smart Network Application (SNA)

Objectif

Le système Smart Network Application (SNA) présente une vue d'ensemble de la topologie du réseau, y compris des informations de surveillance détaillées pour les périphériques et le trafic. SNA permet d'afficher et de modifier globalement les configurations sur tous les périphériques pris en charge sur le réseau.

SNA comporte une fonction appelée DAC (Device Authorization Control) qui vous permet de configurer une liste de périphériques clients autorisés sur le réseau. DAC active les fonctionnalités 802.1X sur les périphériques SNA du réseau et un serveur RADIUS (Remote Authentication Dial-In User Service) ou RADIUS Host Server intégré peut être configuré sur l'un des périphériques SNA. Le contrôle d'accès au support (DAC) est effectué via l'authentification MAC (Media Access Control).

Cet article explique comment configurer la gestion DAC via SNA.

Périphériques pertinents

- Gamme Sx350
- Gamme SG350X
- Gamme Sx550X

Note: Les périphériques de la gamme Sx250 peuvent fournir des informations SNA lorsqu'ils sont connectés au réseau, mais SNA ne peut pas être lancé à partir de ces périphériques.

Version du logiciel

- 2.2.5.68

Workflow DAC

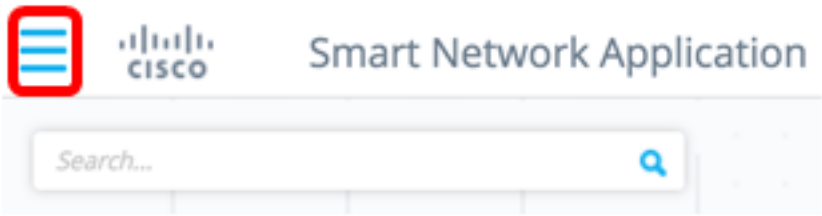
Vous pouvez configurer la gestion DAC en procédant comme suit :

- Activer DAC
- Configuration du serveur et des clients RADIUS
- Gestion des listes DAC

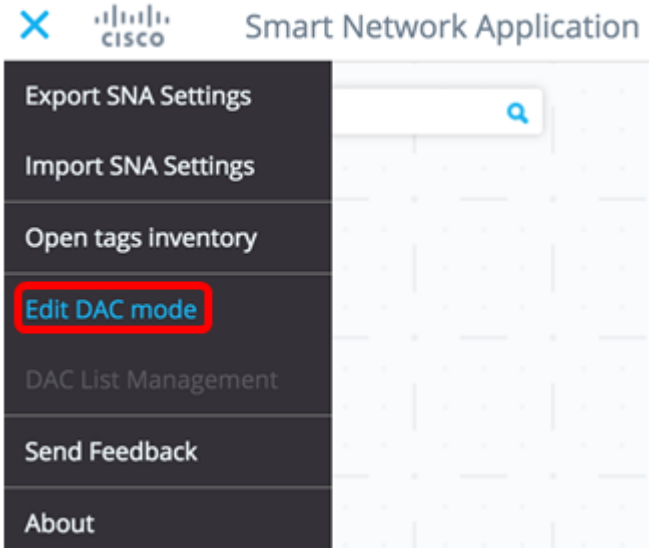
Activer DAC

Pour accéder à DAC et l'activer, procédez comme suit :

Étape 1. Cliquez sur le menu **Options** dans le coin supérieur gauche de la page SNA pour afficher les options disponibles.



Étape 2. Sélectionnez **Modifier le mode DAC**.

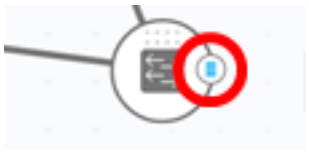


Le mode DAC Edit est maintenant activé. Vous devez voir le cadre bleu sous la carte topologique et le panneau de configuration en bas de l'écran.

Étape 3. (Facultatif) Pour quitter le mode de modification DAC, cliquez sur le bouton **Quitter**.

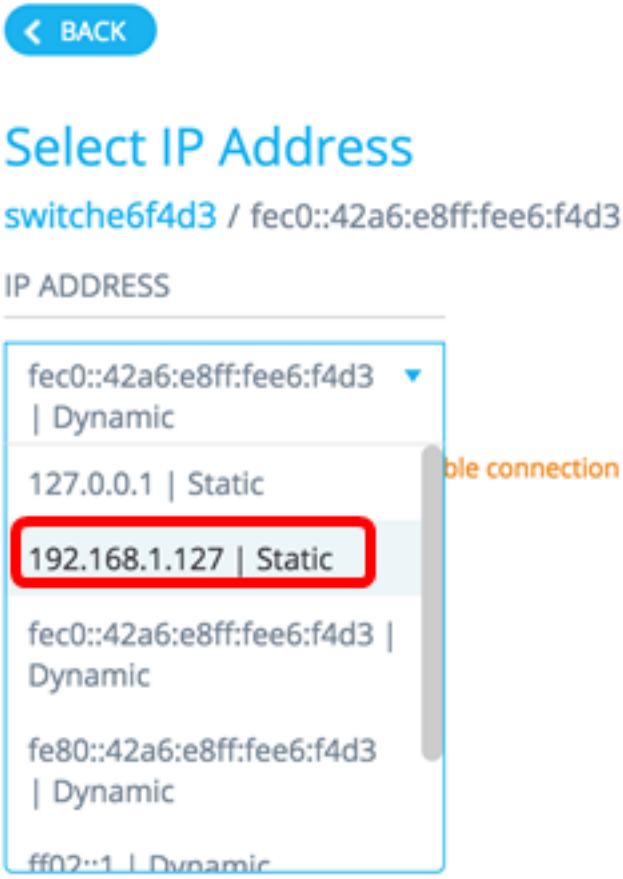
Configuration du serveur et des clients RADIUS

Étape 1. Dans la vue Topologie, sélectionnez l'un des périphériques SNA et cliquez sur son menu **Options**.



Étape 2. Cliquez sur **+ Définir comme serveur DAC**.

Étape 3. Si le périphérique a plusieurs adresses IP, choisissez l'une de ces adresses comme adresse à utiliser par le DAC. Dans cet exemple, 192.168.1.127 | Statique est sélectionné.



Note: La liste d'adresses indique si l'interface IP est statique ou dynamique. Vous serez averti que le choix d'une adresse IP dynamique peut entraîner une connexion instable.

Étape 4. Cliquez sur **Done**.

Note: Lors de la modification d'un serveur DAC existant, l'adresse actuellement utilisée par ses clients est présélectionnée.

Le serveur RADIUS DAC est mis en surbrillance dans la vue Topology.

Étape 5. Choisissez l'un des périphériques SNA et cliquez sur son menu Options.

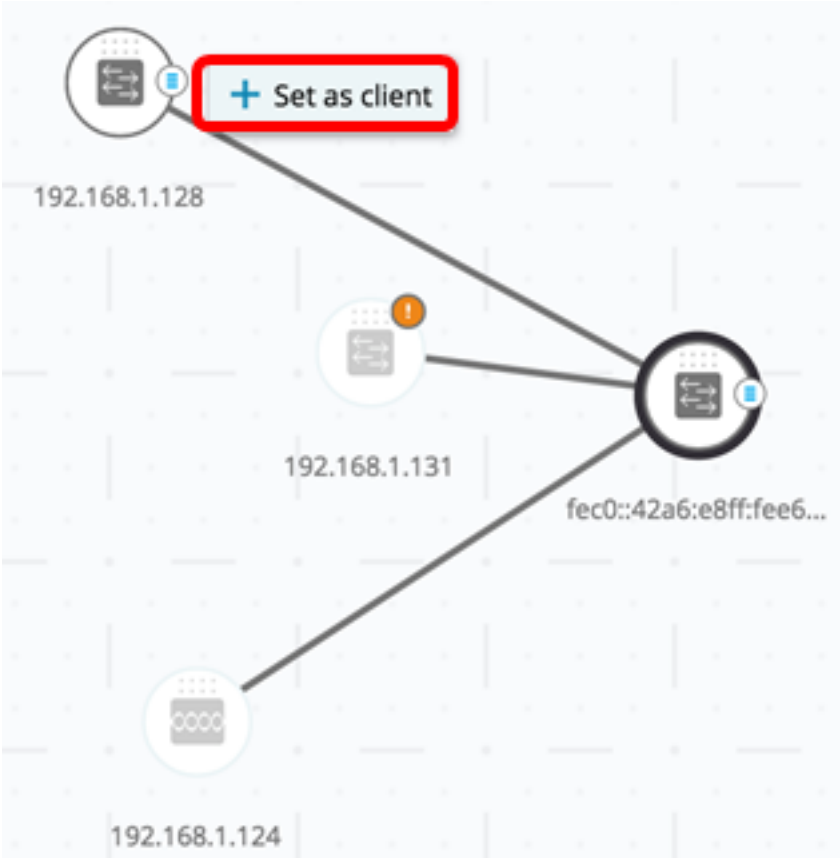
Note: Si aucun client n'est sélectionné, vous ne pourrez pas appliquer les paramètres.

Si un commutateur est déjà un client du serveur RADIUS DAC, son adresse IP se trouve dans la table NAS du serveur RADIUS et le serveur RADIUS est configuré dans sa table de serveur RADIUS avec le type d'utilisation 802.1X ou tout le reste dans la priorité 0. Ce commutateur est présélectionné.

Si un client est choisi, qui a déjà un serveur RADIUS configuré pour 802.1X autre que le serveur précédemment sélectionné, vous serez averti que le processus interrompra le fonctionnement du serveur RADIUS existant.

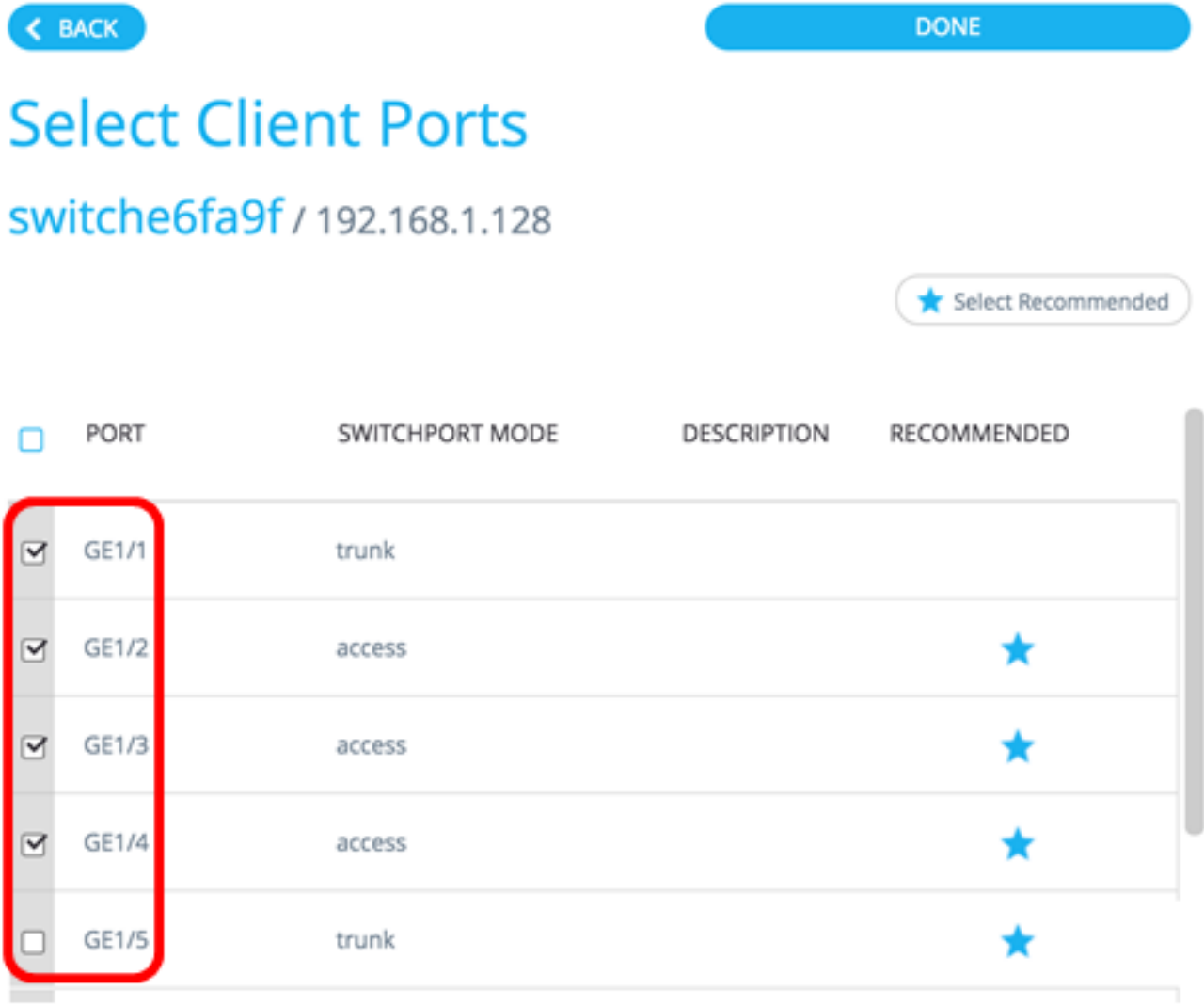
Si un client est choisi, qui a un serveur RADIUS configuré pour 802.1X dans la priorité 0 autre que le serveur précédemment sélectionné, un message d'erreur s'affiche et DAC n'est pas configuré sur ce client.

Étape 6. Cliquez sur **+ Définir comme client**.



Étape 7. Cochez la ou les cases du ou des ports du commutateur client pour appliquer les authentifications 802.1X.

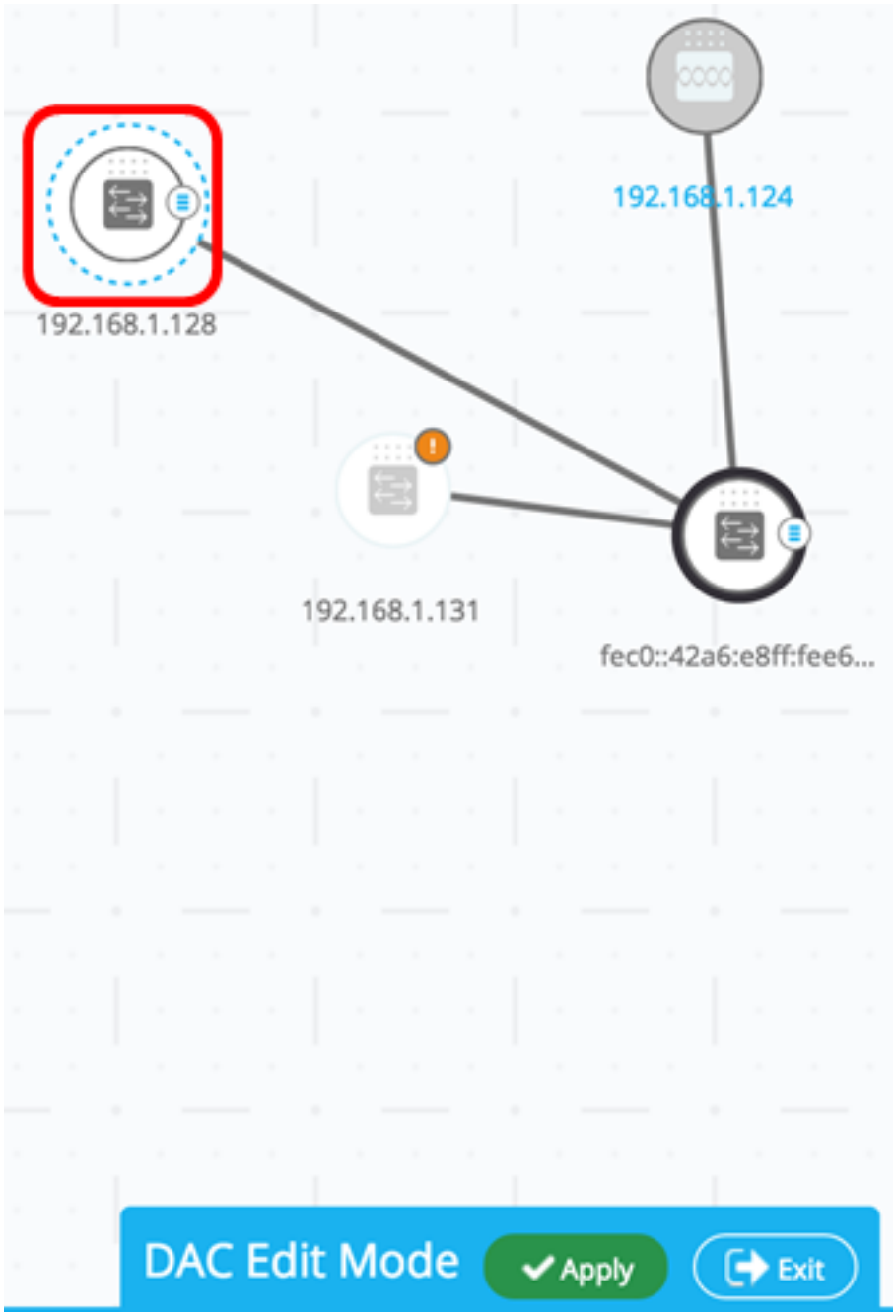
Note: Dans cet exemple, les ports GE1/1, GE1/2, GE1/3 et GE1/4 sont vérifiés.



Note: Le SNA recommande une liste de tous les ports de périphérie ou de tous les ports qui ne sont pas connus pour être connectés à d'autres commutateurs ou clouds.

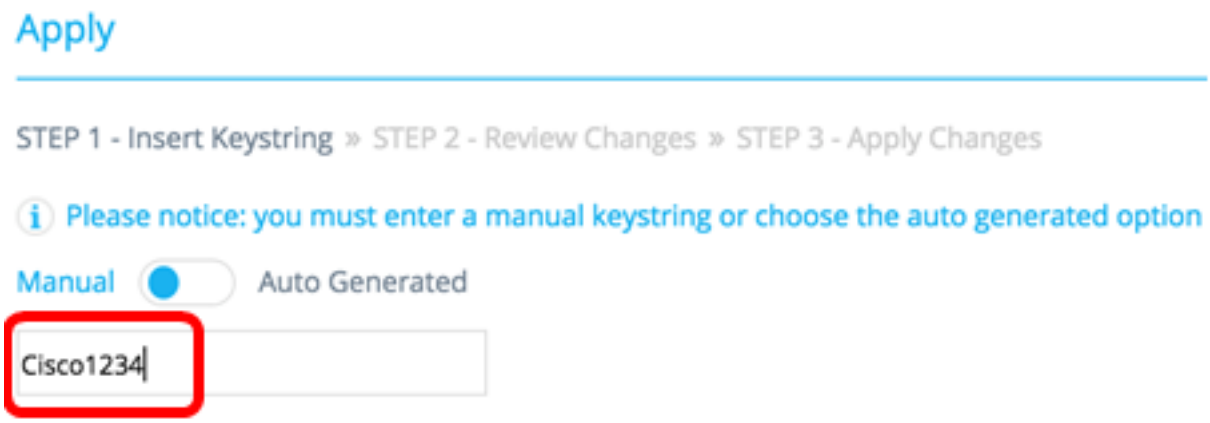
Étape 8. (Facultatif) Cliquez sur le bouton **Sélectionner recommandé** pour vérifier tous les ports recommandés.

Étape 9. Cliquez sur **Done**. Le client RADIUS DAC est mis en surbrillance en bleu pointillé dans la vue Topologie.



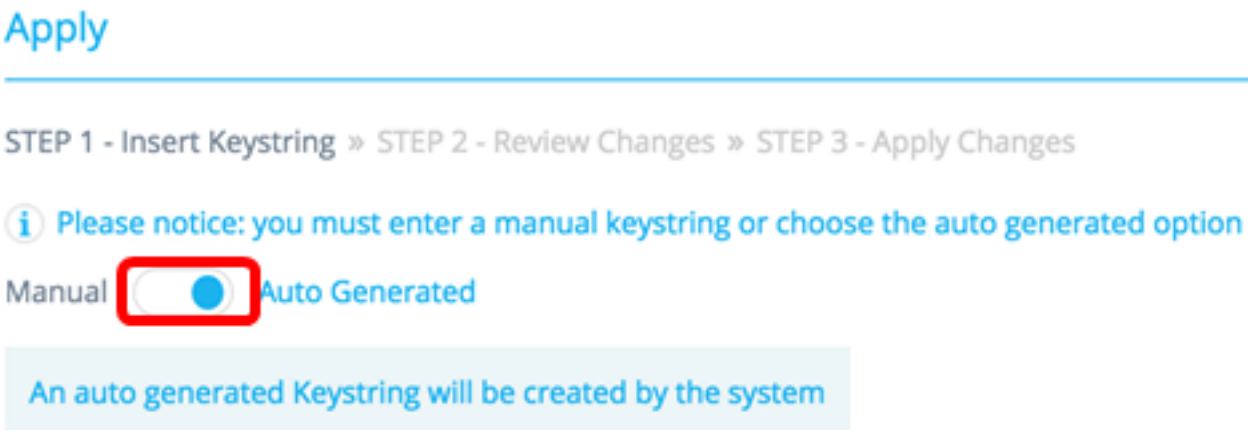
Étape 10. Cliquez sur **Apply** pour enregistrer les modifications.

Étape 11. Entrez une chaîne de clés qui sera utilisée par le serveur RADIUS DAC avec tous ses clients sur le réseau.



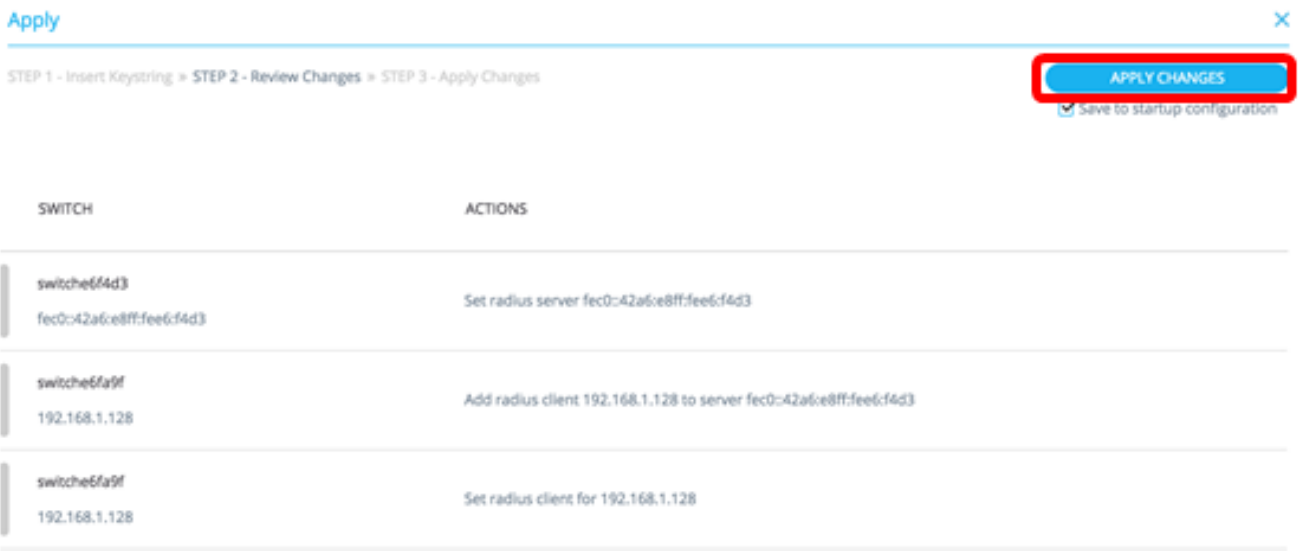
Note: Dans cet exemple, Cisco1234 est utilisé.

Étape 12. (Facultatif) Activez le bouton sur **Généré automatiquement** pour utiliser une chaîne de clés générée automatiquement.



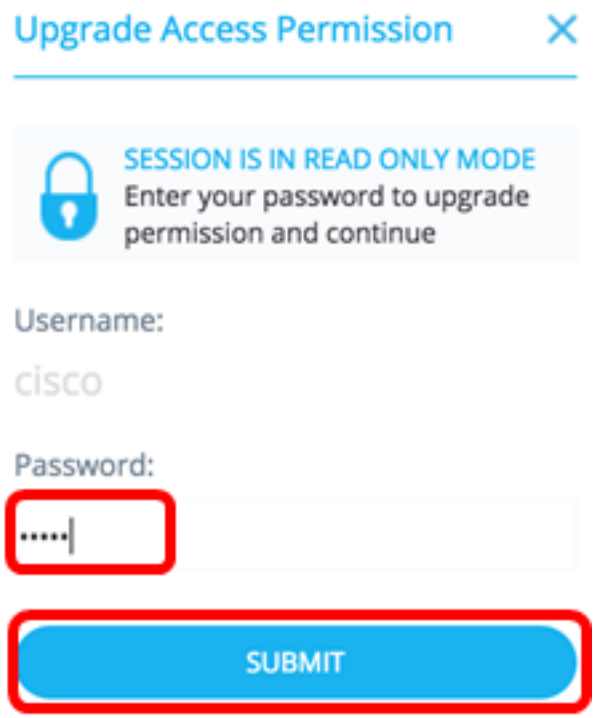
Étape 13. Cliquez sur **Continuer** dans le coin supérieur droit de la page.

Étape 14. Vérifiez les modifications, puis cliquez sur **APPLIQUER LES MODIFICATIONS**.

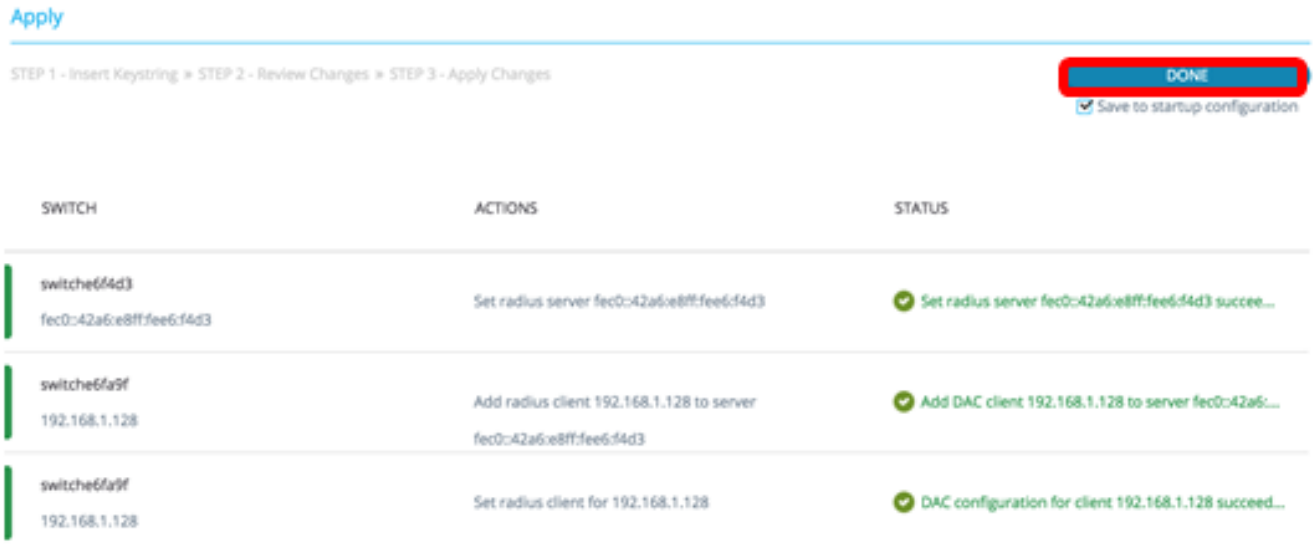


Étape 15. (Facultatif) Décochez la case **Enregistrer dans la configuration initiale** si vous ne souhaitez pas enregistrer les paramètres dans le fichier de configuration.

Étape 16. (Facultatif) Si vous utilisez un compte en lecture seule, vous pouvez être invité à saisir vos informations d'identification pour continuer. Entrez le mot de passe dans le champ *Mot de passe*, puis cliquez sur **SUBMIT**.



Étape 17. La colonne Status doit contenir des cases à cocher vertes qui confirment l'application réussie des modifications. Cliquez sur **Done**.



Une fois le DAC configuré, une alerte s'affiche chaque fois qu'un nouveau périphérique non bloqué est rejeté sur le réseau via un serveur RADIUS compatible DAC. Vous serez invité à ajouter ce périphérique à la liste des périphériques autorisés ou à l'envoyer dans une liste de blocage afin que vous ne soyez plus averti.

Lorsque l'utilisateur est informé du nouveau périphérique, SNA fournit l'adresse MAC du périphérique et le port auquel le périphérique a tenté d'accéder au réseau.

Si un événement de rejet est reçu d'un périphérique qui n'est pas un serveur RADIUS DAC, le message est ignoré et tous les autres messages de ce périphérique pendant les 20 prochaines minutes sont ignorés. Au bout de 20 minutes, SNA vérifie à nouveau si le périphérique est un serveur RADIUS DAC. Si un utilisateur est ajouté à la liste verte, le périphérique est ajouté au groupe DAC de tous les serveurs DAC. Lorsque cette configuration est enregistrée, vous pouvez choisir d'enregistrer ce paramètre immédiatement dans la configuration de démarrage du serveur. Cette option est sélectionnée par défaut.

Tant qu'un périphérique n'est pas ajouté à la liste verte, il n'est pas autorisé à accéder au réseau. Vous pouvez afficher et modifier les listes d'autorisation et de blocage à tout moment, à condition qu'un serveur RADIUS DAC soit défini et accessible. Pour configurer la gestion des listes DAC, passez à Gestion des listes DAC.

Lors de l'application des paramètres DAC, un rapport répertorie les actions qui seront appliquées aux périphériques participants. Après avoir approuvé les modifications, vous pouvez décider si les paramètres doivent être copiés dans le fichier de configuration initiale des périphériques configurés. Enfin, appliquez les configurations.

Le rapport affiche des avertissements si certaines étapes du processus de configuration DAC sont manquantes, ainsi que l'état des actions traitées par les périphériques.

Champ	Valeur	Commentaires
Périphérique	Identificateurs de périphérique (nom d'hôte ou adresse IP)	
Action	Actions possibles pour le serveur DAC : • Activer le serveur RADIUS • Désactiver le serveur RADIUS • Mettre à jour la liste des clients • Créer un groupe de serveurs RADIUS • Supprimer le groupe de serveurs RADIUS Actions possibles pour le client DAC : • Ajouter une connexion au serveur RADIUS • Mettre à jour la connexion du serveur RADIUS • Supprimer la connexion au serveur RADIUS • Mettre à jour les paramètres 802.1x • Mettre à jour les paramètres d'authentification de l'interface • Mettre à jour les paramètres d'hôte et de session de l'interface	Il est possible (et probable) que plusieurs actions apparaissent pour chaque périphérique. Chaque action peut avoir son propre statut.
Avertissements	Les avertissements possibles pour le serveur DAC sont les suivants :	Les avertissements contiennent également des liens vers les sections du CAD où ils peuvent être adressés.

	• L'interface IP sélectionnée est dynamique. Les avertissements possibles pour les clients DAC sont les suivants : • Le périphérique est déjà un client d'un serveur RADIUS différent. • Aucun port n'est sélectionné.	Des modifications peuvent être appliquées en cas de présence d'avertissements.
Status (état)	• En attente • Réussite • Échec	Lorsque l'état est défaillant, le message d'erreur s'affiche pour l'action.

Gestion des listes DAC

Une fois que vous avez ajouté des périphériques clients et sélectionné lesquels de leurs ports doivent être authentifiés, tous les périphériques non authentifiés détectés sur ces ports sont ajoutés à la liste Unauthenticated Devices.

DAC prend en charge les listes de périphériques suivantes :

- Allow List : contient la liste de tous les clients pouvant être authentifiés.
- Block List : **contient** la liste des clients qui ne doivent jamais être authentifiés.

Si vous voulez que les périphériques et leurs ports soient authentifiés, ils doivent être ajoutés aux listes d'autorisation. Si vous ne voulez pas qu'ils soient authentifiés, aucune action n'est requise car ils seront ajoutés à la liste de blocage par défaut.

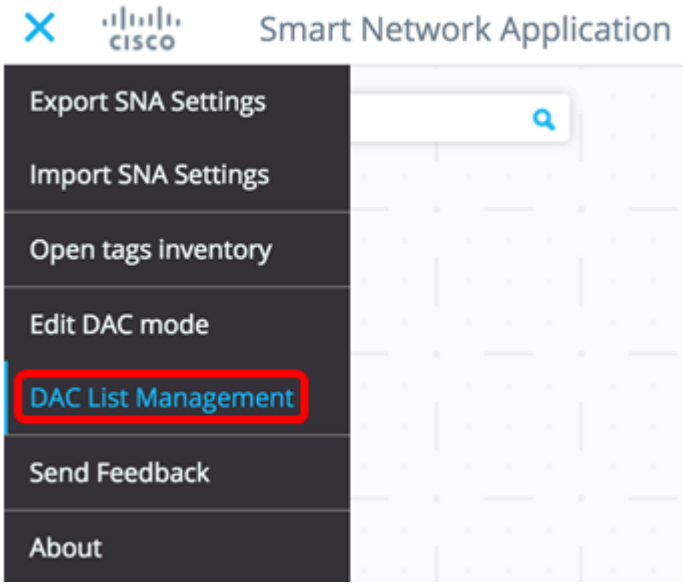
Pour plus d'informations, reportez-vous au glossaire.

Ajouter des périphériques à la liste Autoriser ou Bloquer

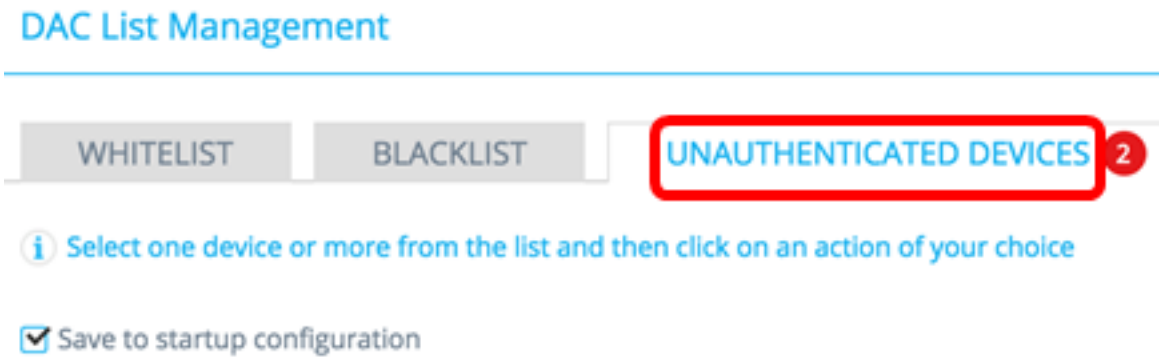
Pour ajouter des périphériques à la liste d'autorisation ou de blocage, procédez comme suit :

Étape 1. Cliquez sur le menu **Options** dans le coin supérieur gauche de la page SNA pour afficher les options disponibles.

Étape 2. Sélectionnez **Gestion de la liste DAC**.

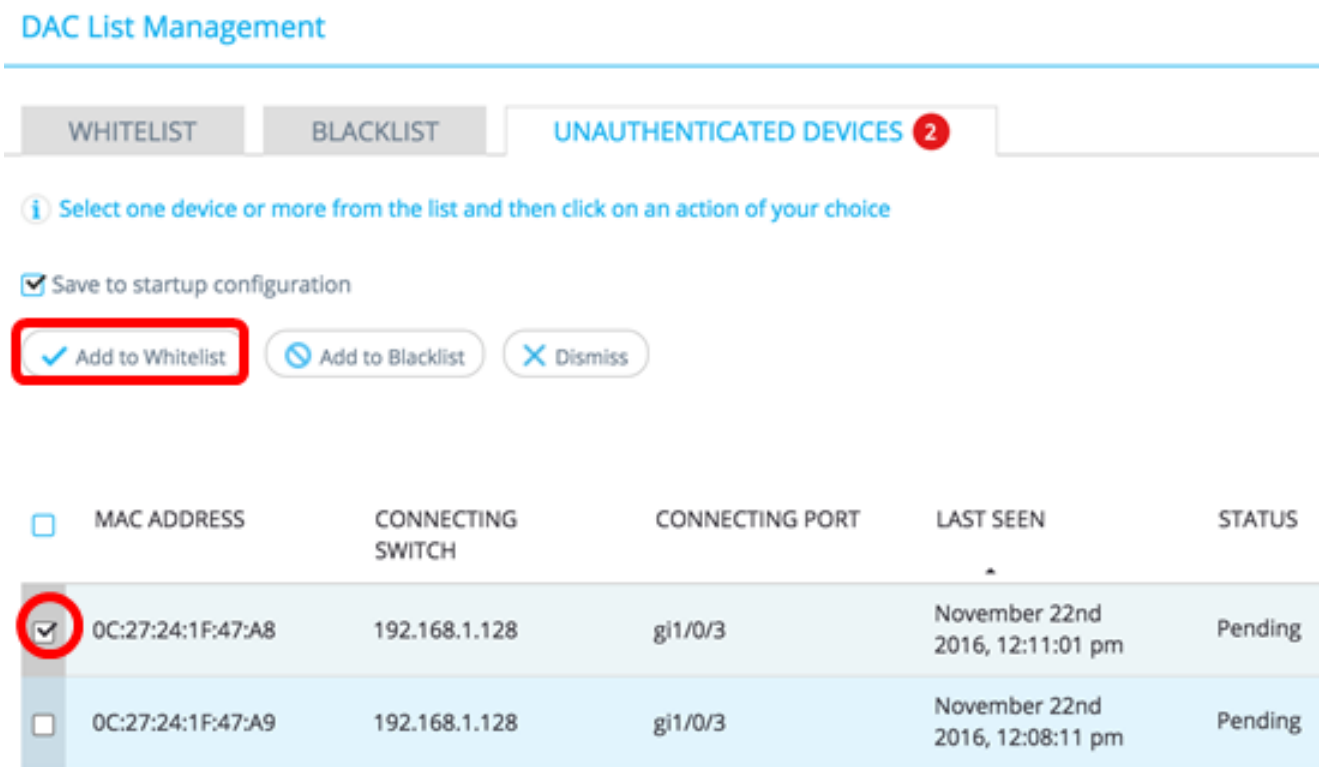


Étape 3. Cliquez sur l'onglet **PÉRIPHÉRIQUES NON AUTHENTIFIÉS**. Cette page affiche la liste de tous les périphériques non authentifiés.

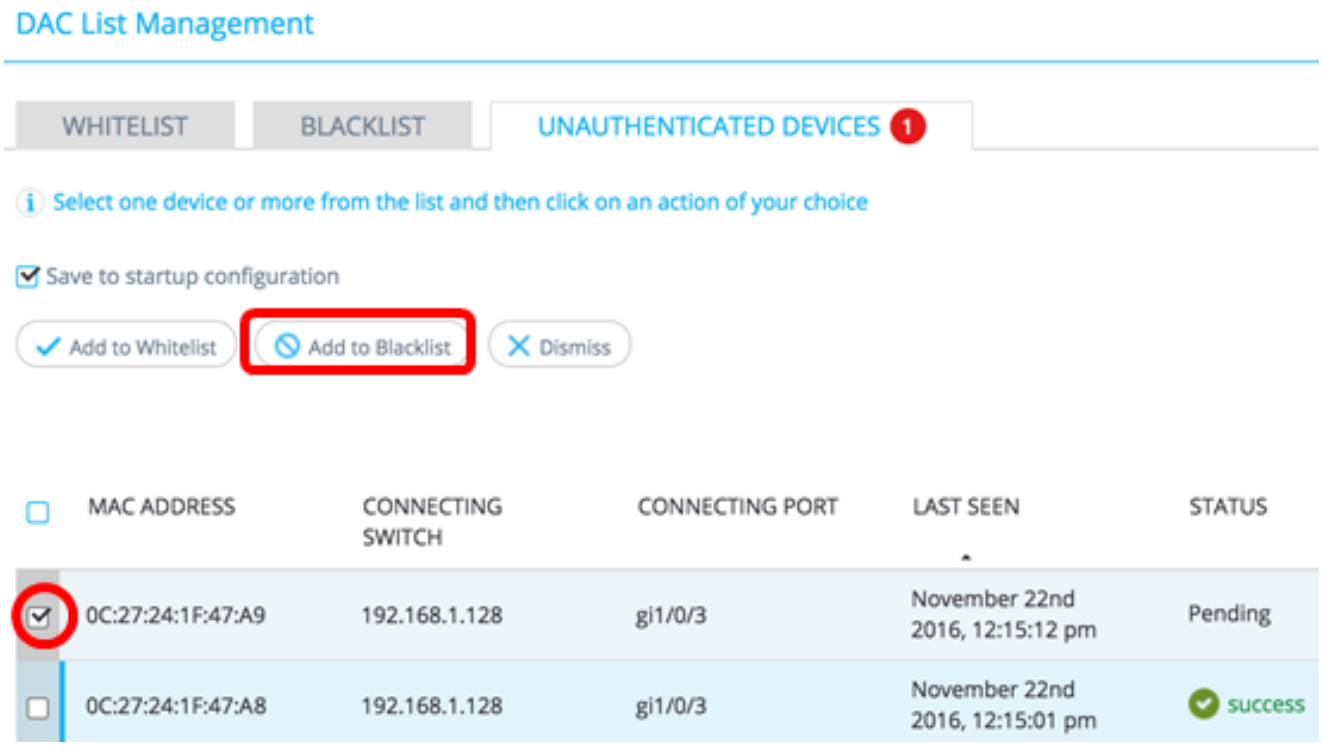


Note: Vous pouvez également cliquer sur l'icône DAC List Management System dans l'angle supérieur droit de la page SNA.

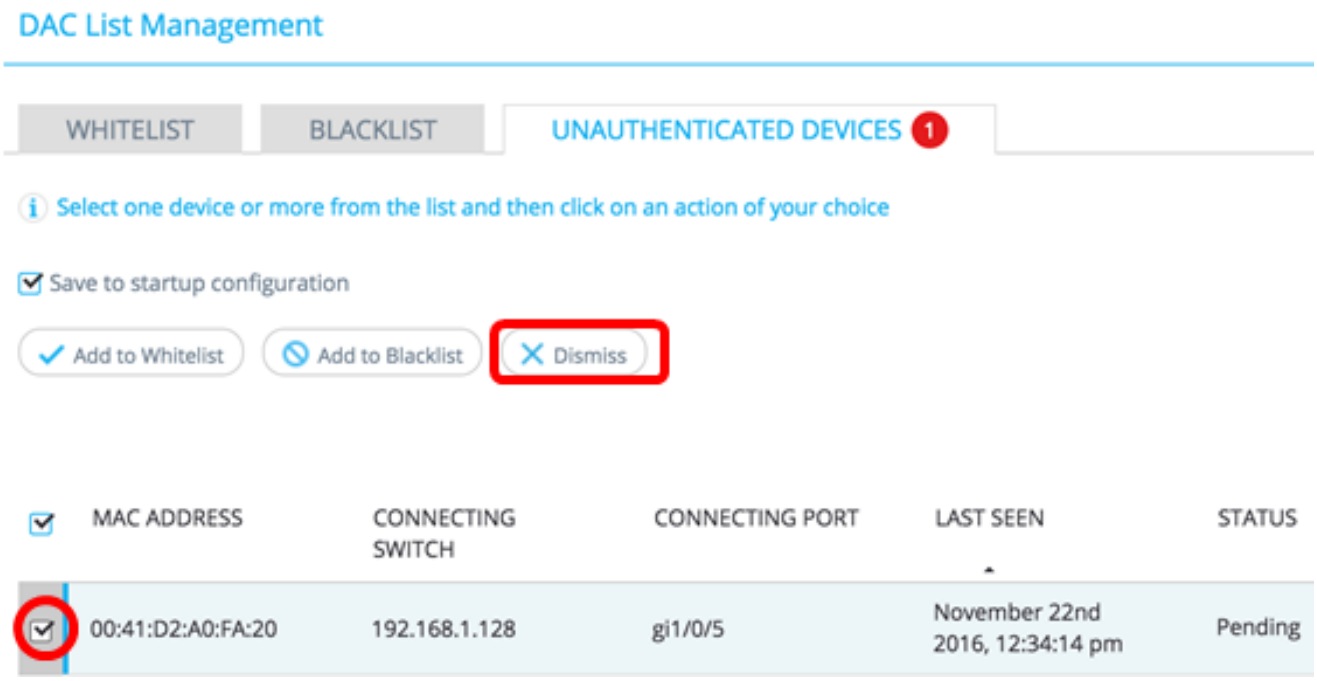
Étape 4. (Facultatif) Cochez la case en regard de l'adresse MAC du ou des périphériques que vous voulez ajouter à la liste verte et cliquez sur **Ajouter à la liste verte**.



Étape 5. (Facultatif) Cochez la case en regard de l'adresse MAC du ou des périphériques à ajouter à la liste de blocage et cliquez sur **Ajouter à la liste de blocage**.



Étape 6. (Facultatif) Cochez la case en regard de l'adresse MAC du ou des périphériques que vous voulez supprimer et cliquez sur **Supprimer**.

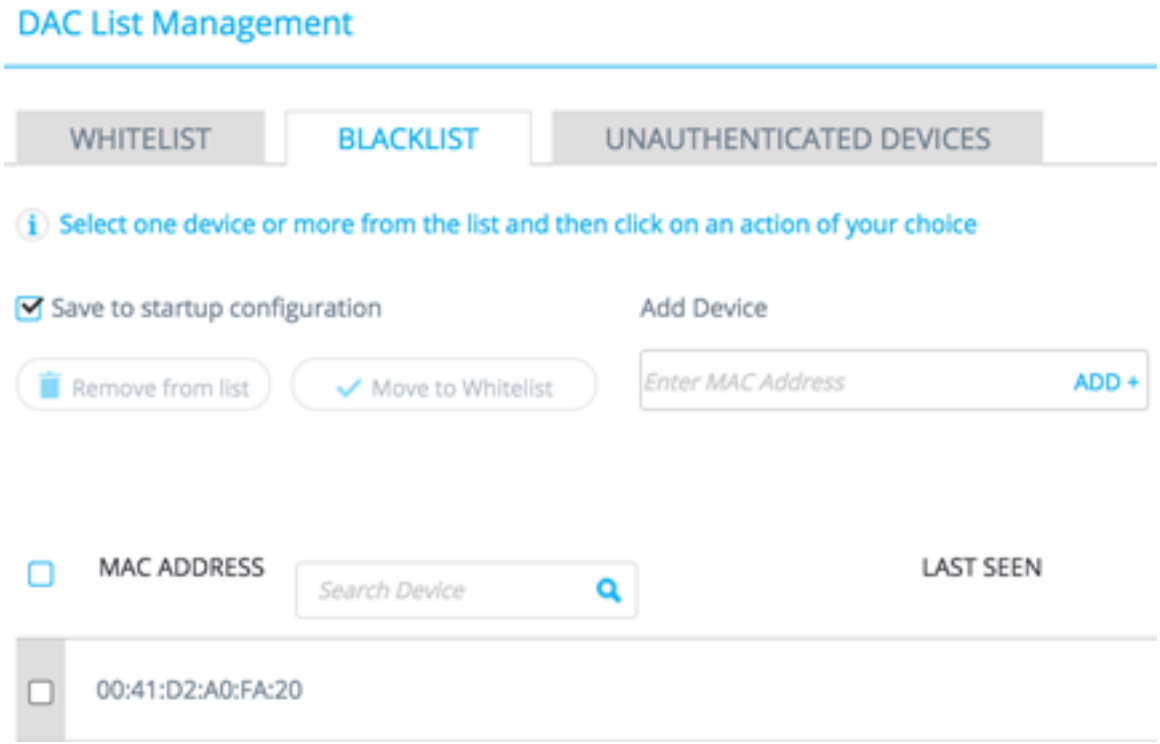


Note: Tous les paquets entrant sur les ports du périphérique sont authentifiés sur le serveur RADIUS.

Vous devez maintenant ajouter un périphérique à la liste Autoriser ou Bloquer.

Gérer les périphériques de la liste Autoriser ou Bloquer

Pour gérer les listes d'autorisation ou de blocage, cliquez sur l'onglet **ALLOW LIST** ou **BLOCK LIST** en conséquence.



Vous pouvez effectuer les tâches suivantes dans ces pages :

- Supprimer de la liste : cette action supprime le ou les périphériques sélectionnés de la liste.
- Déplacer vers la liste Bloquer ou Déplacer vers la liste Autoriser — Cette action déplace le ou

les périphériques sélectionnés vers la liste spécifiée.

- Ajouter un périphérique : cette action ajoute un périphérique à la liste de blocage ou d'autorisation en entrant son adresse MAC et en cliquant sur le bouton **ADD+**.
- Rechercher un périphérique à l'aide d'une adresse MAC : saisissez une adresse MAC et cliquez sur le bouton **Rechercher**  bouton.

Vous devez maintenant gérer les périphériques de la liste DAC.