Configurazione della gestione di Controllo autorizzazione dispositivo (DAC) tramite Smart Network Application (SNA)

Obiettivo

Il sistema SNA (Smart Network Application) visualizza una panoramica della topologia di rete, con informazioni dettagliate sul monitoraggio dei dispositivi e del traffico. La SNA consente di visualizzare e modificare le configurazioni a livello globale su tutti i dispositivi supportati nella rete.

La SNA dispone di una funzionalità nota come DAC (Device Authorization Control) che consente di configurare un elenco di dispositivi client autorizzati nella rete. DAC attiva le funzionalità 802.1X sui dispositivi SNA della rete e un server host RADIUS (Remote Authentication Dial-In User Service) incorporato può essere configurato su uno dei dispositivi SNA. L'applicazione livello dati viene eseguita tramite l'autenticazione MAC (Media Access Control).

In questo documento viene spiegato come configurare Gestione applicazione livello dati tramite SNA.

Dispositivi interessati

- Serie Sx350
- Serie SG350X
- Serie Sx550X

Nota: I dispositivi della serie Sx250 possono fornire informazioni SNA quando sono collegati alla rete, ma non è possibile avviare SNA da questi dispositivi.

Versione del software

- 2.2.5.68

Flusso di lavoro DAC

Èpossibile configurare la gestione dell'applicazione livello dati eseguendo la procedura seguente:

- Attiva DAC
- Configurazione server e client RADIUS
- Gestione elenchi DAC

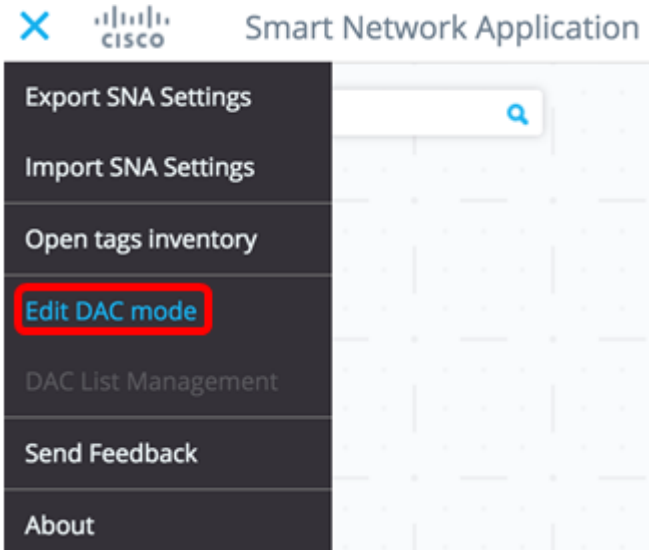
Attiva DAC

Per accedere e attivare DAC, eseguire la procedura seguente:

Passaggio 1. Per visualizzare le opzioni disponibili, fare clic sul menu **Opzioni** nell'angolo

superiore sinistro della pagina SNA.

Passaggio 2. Scegliere **Modifica modalità applicazione livello dati**.



La modalità di modifica DAC è attivata. Nella parte inferiore dello schermo verrà visualizzato il riquadro blu sotto la mappa topologica e il pannello di controllo.

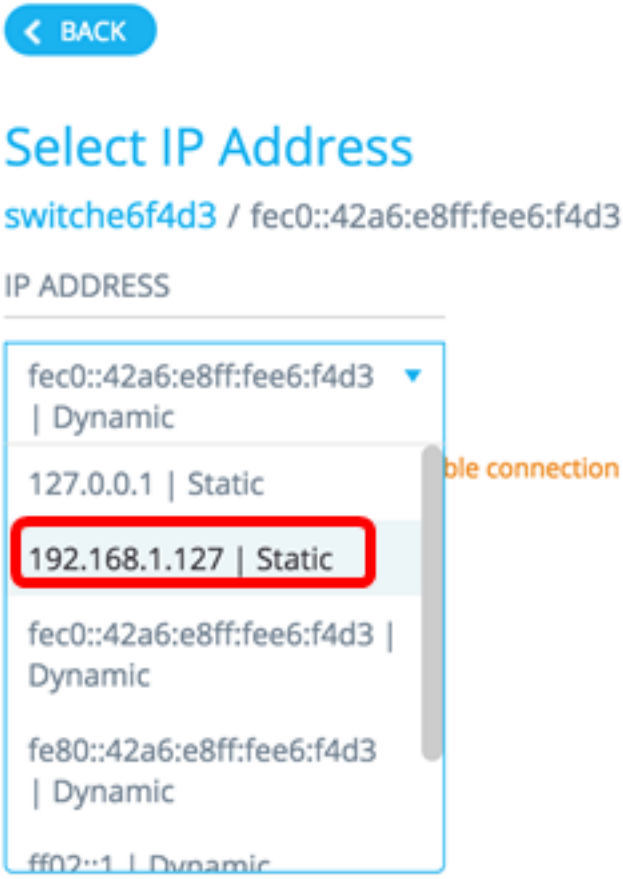
Passaggio 3. (Facoltativo) Per uscire dalla modalità di modifica applicazione livello dati, fare clic sul pulsante **Esci**.

Configurazione server e client RADIUS

Passaggio 1. Nella vista Topologia, scegliere una delle periferiche SNA e fare clic sul relativo menu **Opzioni**.

Passaggio 2. Fare clic su **+ Imposta come server DAC**.

Passaggio 3. Se il dispositivo dispone di più indirizzi IP, scegliere uno di questi come indirizzo da utilizzare per DAC. Nell'esempio, 192.168.1.127 Si sceglie Static.



Nota: L'elenco di indirizzi indica se l'interfaccia IP è statica o dinamica. Viene visualizzato un messaggio di avvertenza per avvertire che la scelta di un indirizzo IP dinamico potrebbe causare instabilità nella connessione.

Passaggio 4. Fare clic su **FINE**.

Nota: Quando si modifica un server DAC esistente, l'indirizzo attualmente utilizzato dai relativi client viene preselezionato.

Il server RADIUS DAC viene evidenziato in solido nella vista Topologia.

Passaggio 5. Scegliere uno dei dispositivi SNA e fare clic sul menu Opzioni.

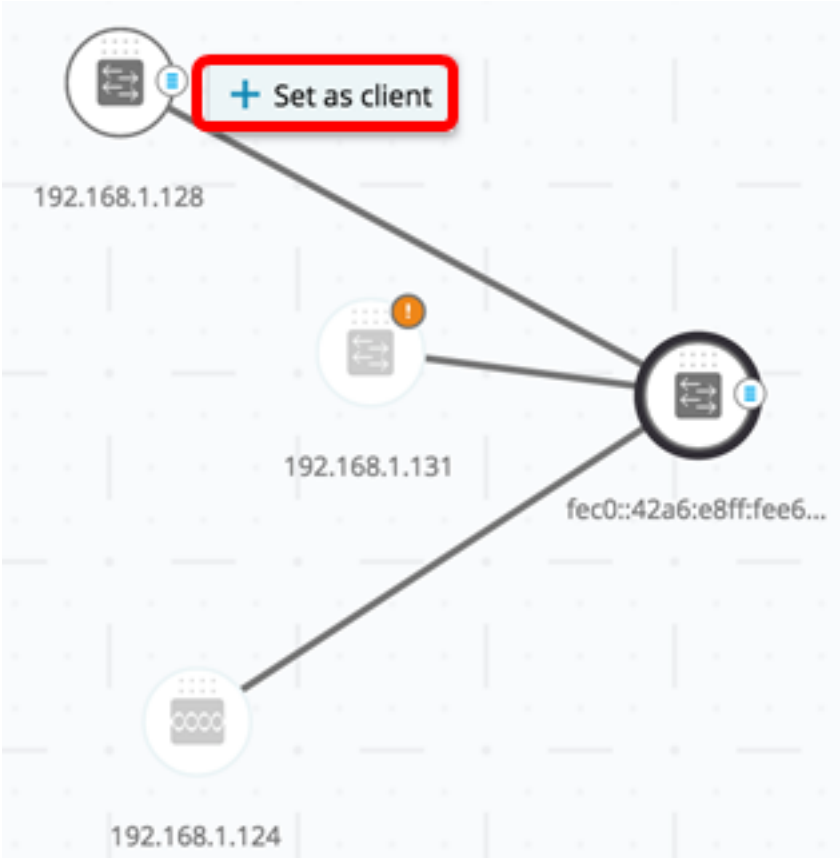
Nota: Se non è selezionato alcun client, non sarà possibile applicare le impostazioni.

Se uno switch è già un client del server RADIUS DAC, il relativo indirizzo IP si trova nella tabella NAS del server RADIUS e quest'ultimo è configurato nella relativa tabella del server RADIUS con il tipo di utilizzo 802.1X o tutti con priorità 0. Questo switch è preselezionato.

Se si sceglie un client per il quale è già stato configurato un server RADIUS per 802.1X diverso dal server selezionato in precedenza, verrà visualizzato un messaggio che informa che la procedura interromperà l'operazione del server RADIUS esistente.

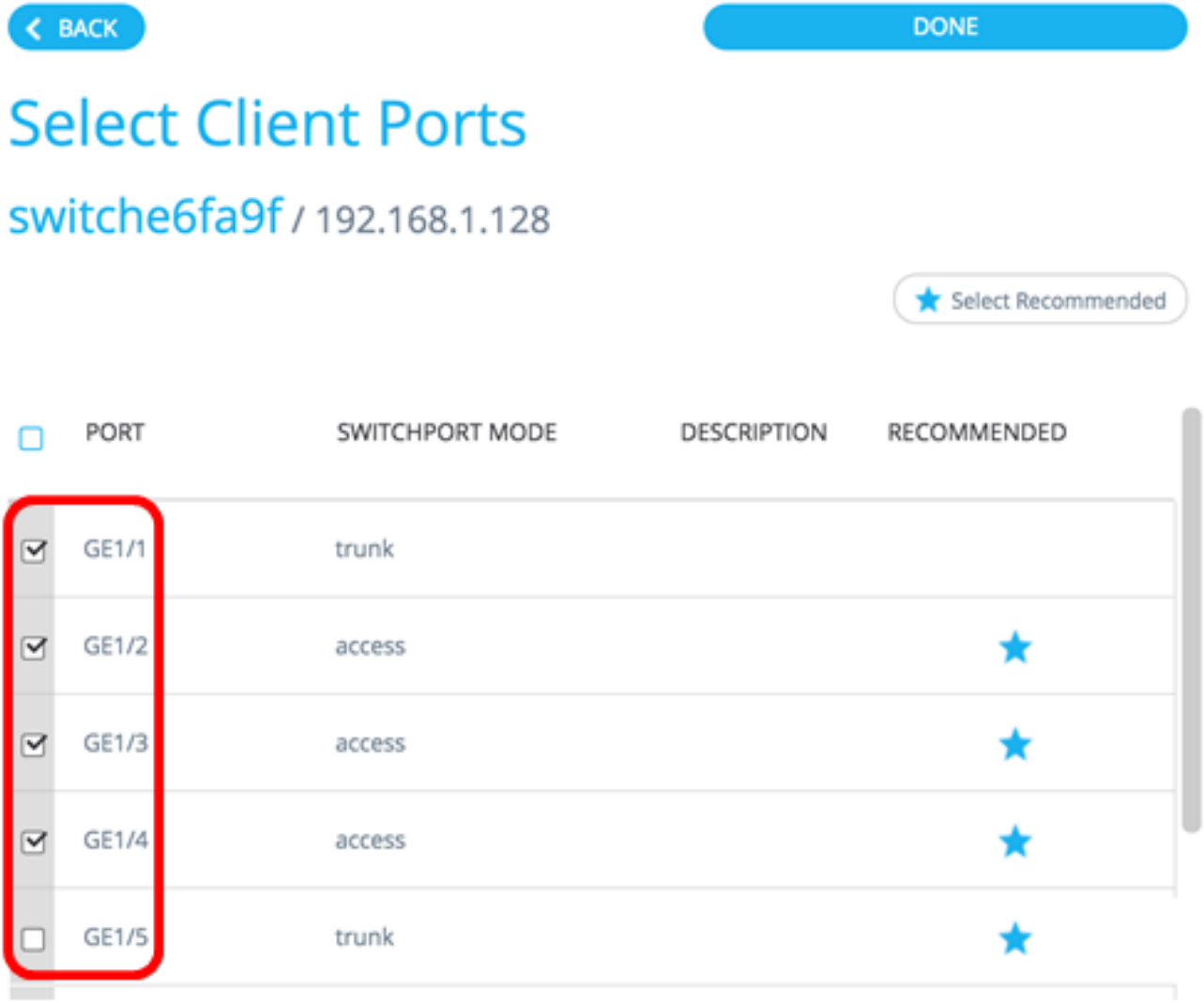
Se si sceglie un client per il quale è configurato un server RADIUS per 802.1X con priorità 0 diverso dal server selezionato in precedenza, viene visualizzato un messaggio di errore e l'applicazione livello dati non è configurata nel client.

Passaggio 6. Fare clic su **+ Imposta come client**.



Passaggio 7. Selezionare la casella o le caselle di controllo della porta o delle porte dello switch client per applicare le autenticazioni 802.1X.

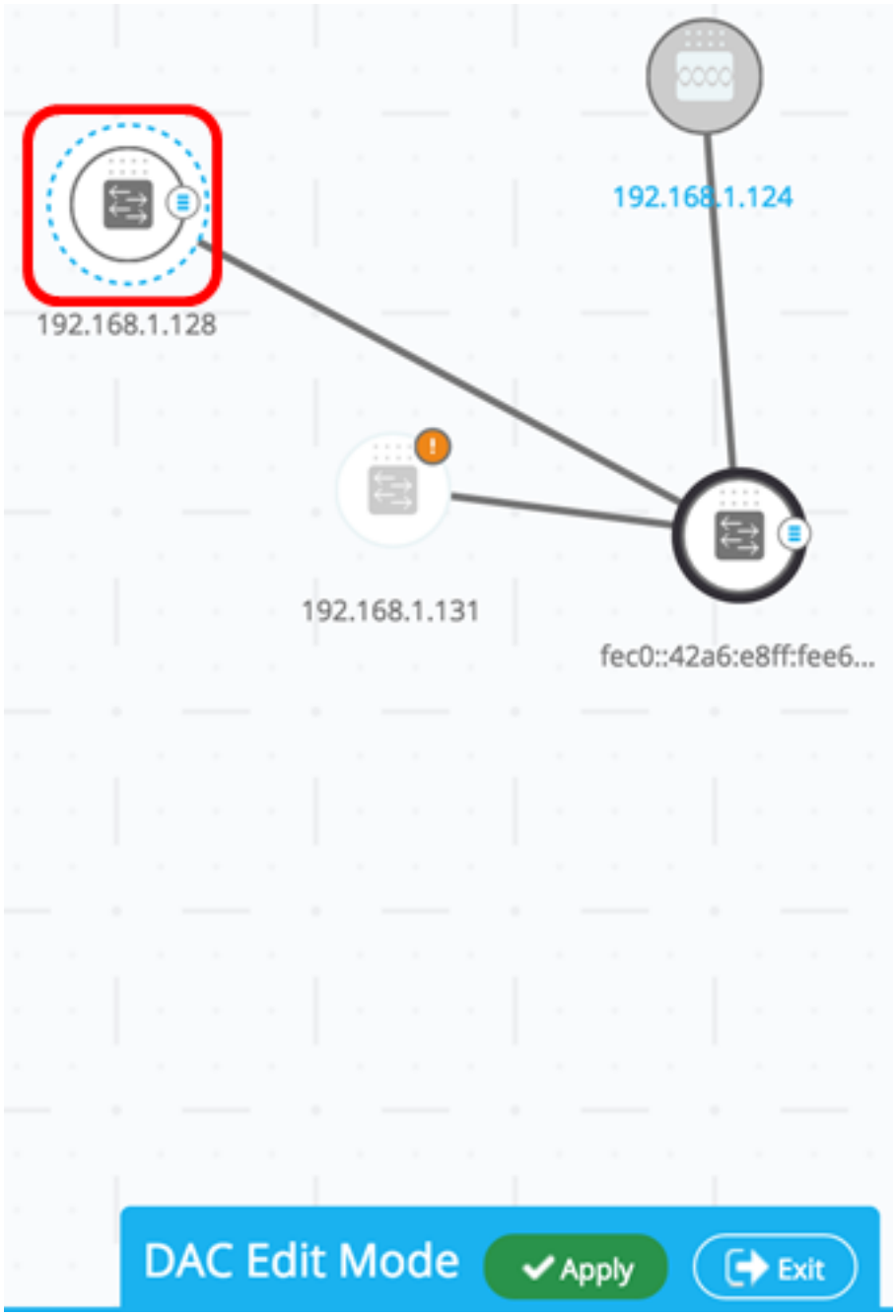
Nota: Nell'esempio, vengono controllate le porte GE1/1, GE1/2, GE1/3 e GE1/4.



Nota: La SNA consiglia un elenco di tutte le porte perimetrali o di tutte le porte che non sono note per essere connesse ad altri switch o cloud.

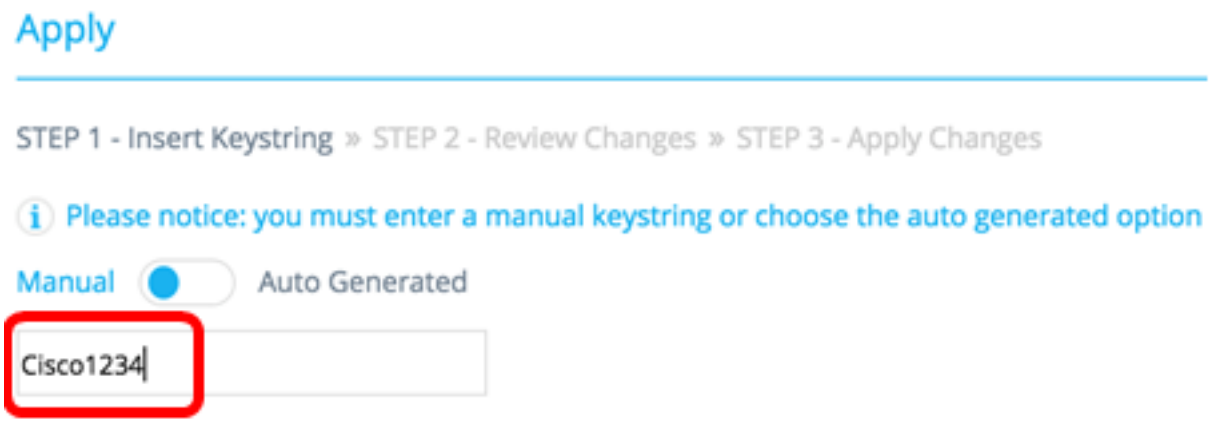
Passaggio 8. (Facoltativo) Fare clic sul pulsante **Seleziona consigliati** per controllare tutte le porte consigliate.

Passaggio 9. Fare clic su **FINE**. Il client RADIUS DAC viene evidenziato in blu tratteggiato nella vista Topologia.



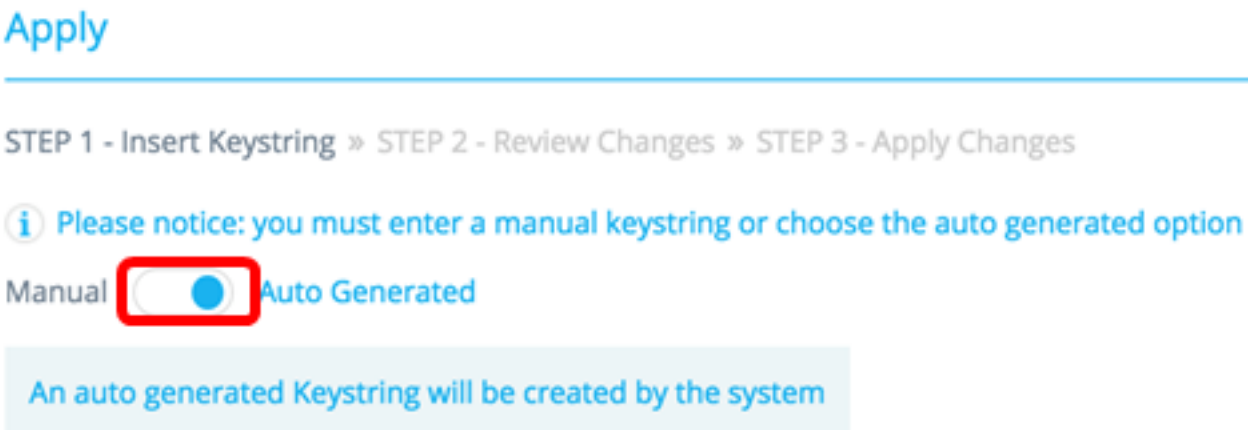
Passaggio 10. Fare clic su **Applica** per salvare le modifiche.

Passaggio 11. Immettere una stringa di chiave che verrà utilizzata dal server RADIUS DAC con tutti i relativi client nella rete.



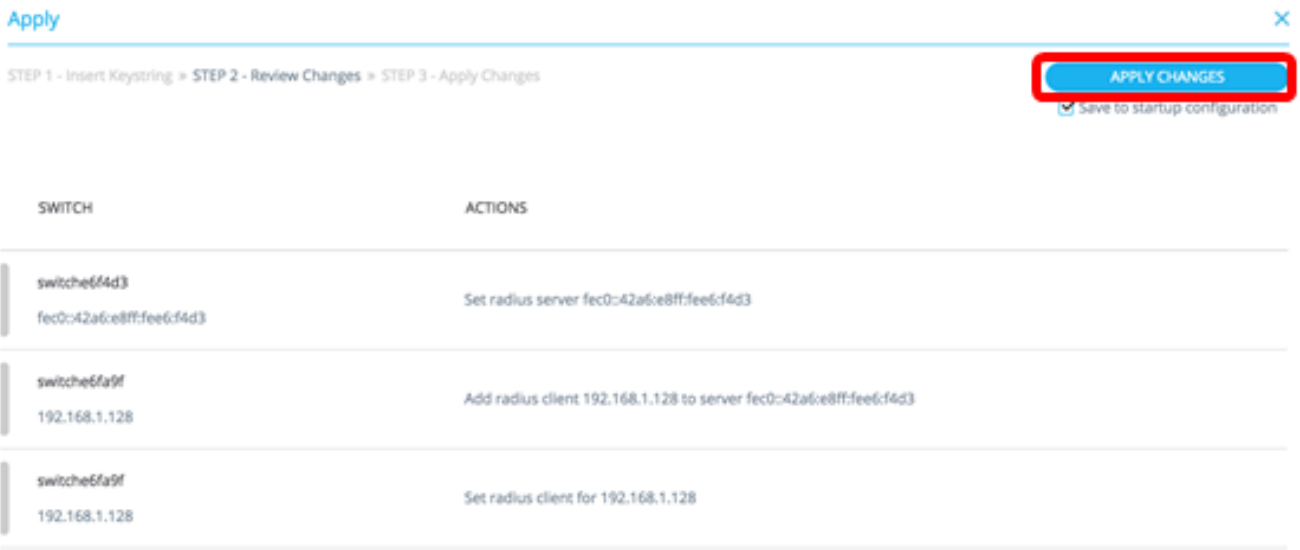
Nota: Nell'esempio viene usato Cisco 1234.

Passaggio 12. (Facoltativo) Impostare il pulsante su **Generato automaticamente** per utilizzare una stringa di chiave generata automaticamente.



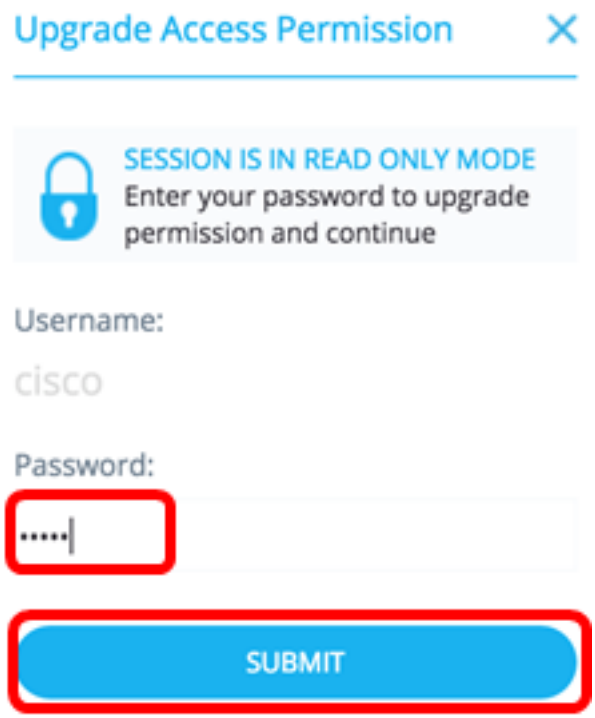
Passaggio 13. Fare clic su **Continua** nell'angolo superiore destro della pagina.

Passaggio 14. Esaminare le modifiche, quindi fare clic su **APPLY CHANGES** (APPLICA MODIFICHE).

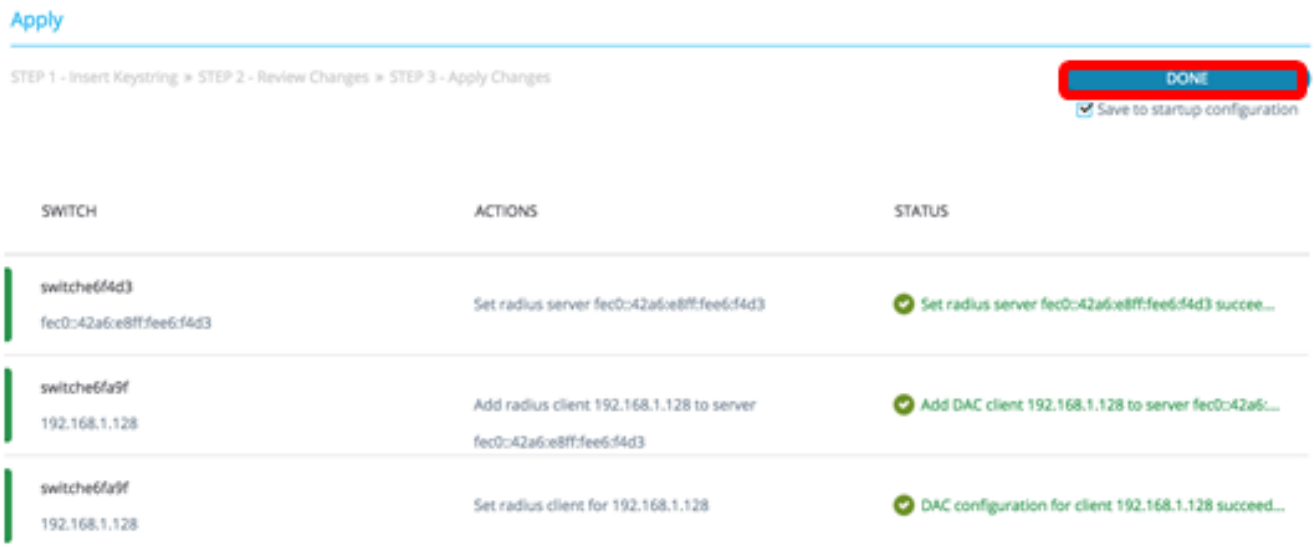


Passaggio 15. (Facoltativo) Deselezionare la casella di controllo **Salva nella configurazione di avvio** se non si desidera salvare le impostazioni nel file di configurazione.

Passaggio 16. (Facoltativo) Se si utilizza un account di sola lettura, è possibile che venga richiesto di immettere le credenziali per continuare. Immettere la password nel campo *Password*, quindi fare clic su **SUBMIT** (INVIA).



Passaggio 17. La colonna Stato deve contenere caselle di controllo verdi che confermano la corretta applicazione delle modifiche. Selezionate **FATTO (DONE)**.



Dopo aver configurato l'applicazione livello dati, verrà visualizzato un avviso ogni volta che un nuovo dispositivo non incluso nell'elenco a blocchi viene rifiutato nella rete tramite un server RADIUS abilitato per l'applicazione livello dati. Verrà richiesto se si desidera aggiungere il dispositivo all'elenco dei dispositivi autorizzati o se si desidera inviarlo a un elenco di dispositivi bloccati in modo che non venga più visualizzato alcun avviso.

Quando si informa l'utente della nuova periferica, la SNA fornisce l'indirizzo MAC della periferica e la porta alla quale la periferica ha tentato di accedere alla rete.

Se si riceve un evento di rifiuto da un dispositivo che non è un server RADIUS DAC, il messaggio verrà ignorato e tutti gli altri messaggi inviati da questo dispositivo per i successivi 20 minuti verranno ignorati. Dopo 20 minuti, l'SNA verifica nuovamente se il dispositivo è un server RADIUS DAC. Se un utente viene aggiunto all'elenco Consenti, il dispositivo verrà aggiunto al gruppo DAC di tutti i server DAC. Quando si salva questa configurazione, è possibile scegliere se salvare immediatamente l'impostazione nella configurazione di avvio del server. Questa opzione è selezionata per default.

L'accesso alla rete non è consentito fino a quando un dispositivo non viene aggiunto all'elenco dei dispositivi consentiti. È possibile visualizzare e modificare gli elenchi Consenti e Blocca in qualsiasi momento, purché sia definito e raggiungibile un server RADIUS DAC. Per configurare Gestione elenco applicazione livello dati, passare a Gestione elenco applicazione livello dati.

Quando si applicano le impostazioni DAC, viene visualizzato un report che elenca le azioni che verranno applicate ai dispositivi partecipanti. Dopo aver approvato le modifiche, è possibile decidere se copiare le impostazioni nel file della configurazione di avvio dei dispositivi configurati. Infine, applicare le configurazioni.

Il report visualizza avvisi se alcuni passaggi del processo di configurazione DAC non vengono completati, insieme allo stato delle azioni gestite dai dispositivi.

Campo	Valore	Commenti
Sul dispositivo bootflash o slot0:	Gli identificatori di dispositivo (nome host o indirizzo IP)	
Azione	Azioni possibili per il server DAC: • Abilita server RADIUS • Disabilita server RADIUS • Aggiorna elenco client • Crea gruppo di server RADIUS • Elimina gruppo di server RADIUS Azioni possibili per il client DAC: • Aggiungi connessione server RADIUS • Aggiorna connessione server RADIUS • Rimuovi connessione server RADIUS • Aggiorna impostazioni 802.1x • Aggiorna impostazioni di autenticazione interfaccia	Èpossibile (ed è probabile) che per ogni dispositivo vengano visualizzate più azioni. Ogni azione può avere il proprio stato.

	• Aggiorna impostazioni di sessione e host interfaccia	
Avvisi	Gli avvisi possibili per il server DAC includono: • L'interfaccia IP selezionata è dinamica. I possibili avvisi per i client DAC includono: • Il dispositivo è già un client di un server RADIUS diverso. • Nessuna porta selezionata.	Gli avvisi contengono inoltre collegamenti alle sezioni dell'applicazione livello dati a cui possono essere indirizzati. Le modifiche possono essere applicate quando sono presenti avvisi.
Stato	• In sospeso • Riuscito • Errore	Quando lo stato è un errore, viene visualizzato il messaggio di errore relativo all'azione.

Gestione elenchi DAC

Dopo aver aggiunto i dispositivi client e selezionato le porte da autenticare, tutti i dispositivi non autenticati rilevati su tali porte vengono aggiunti all'elenco dei dispositivi non autenticati.

DAC supporta i seguenti elenchi di dispositivi:

- Elenco Consenti — contiene l'elenco di tutti i client che possono essere autenticati.
- Blocca elenco - **contiene** l'elenco dei client che non devono mai essere autenticati.

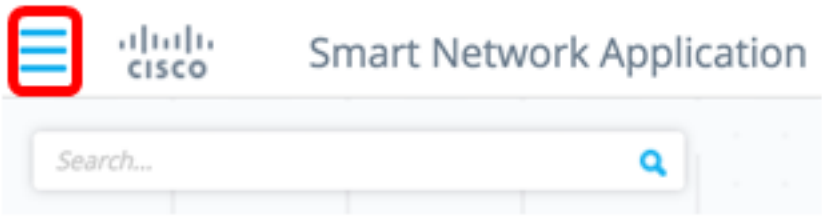
Se si desidera che i dispositivi e le relative porte vengano autenticati, è necessario aggiungerli agli elenchi dei dispositivi consentiti. Se non si desidera che vengano autenticati, non è necessaria alcuna azione poiché verranno aggiunti all'elenco Blocca per impostazione predefinita.

Per ulteriori informazioni, consultare il glossario.

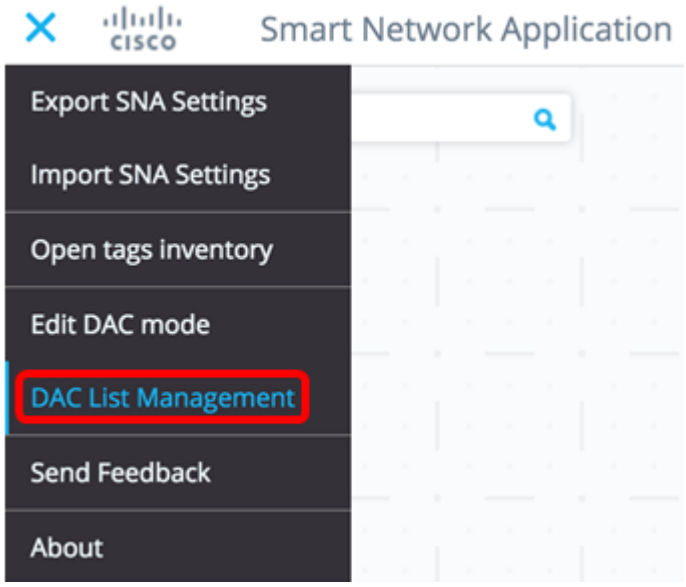
Aggiungi dispositivi all'elenco Consenti o Blocca

Per aggiungere dispositivi all'elenco dei dispositivi consentiti o bloccati, eseguire la procedura seguente:

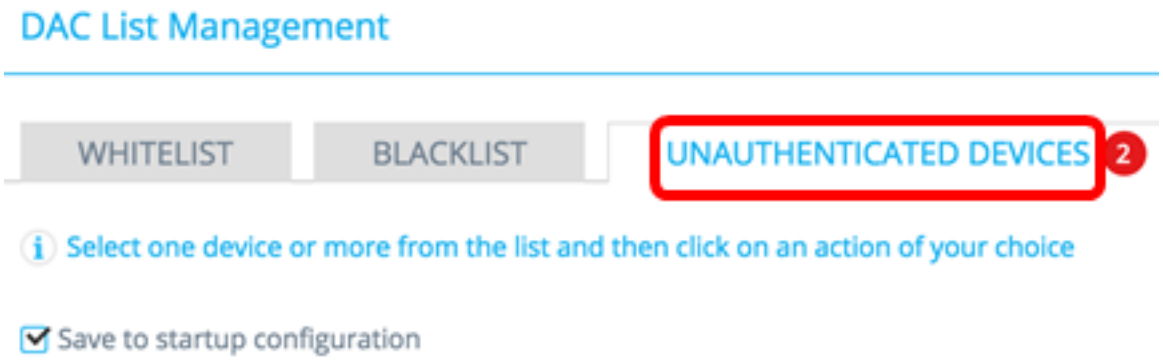
Passaggio 1. Per visualizzare le opzioni disponibili, fare clic sul menu **Opzioni** nell'angolo superiore sinistro della pagina SNA.



Passaggio 2. Scegliere **Gestione elenco applicazione livello dati**.

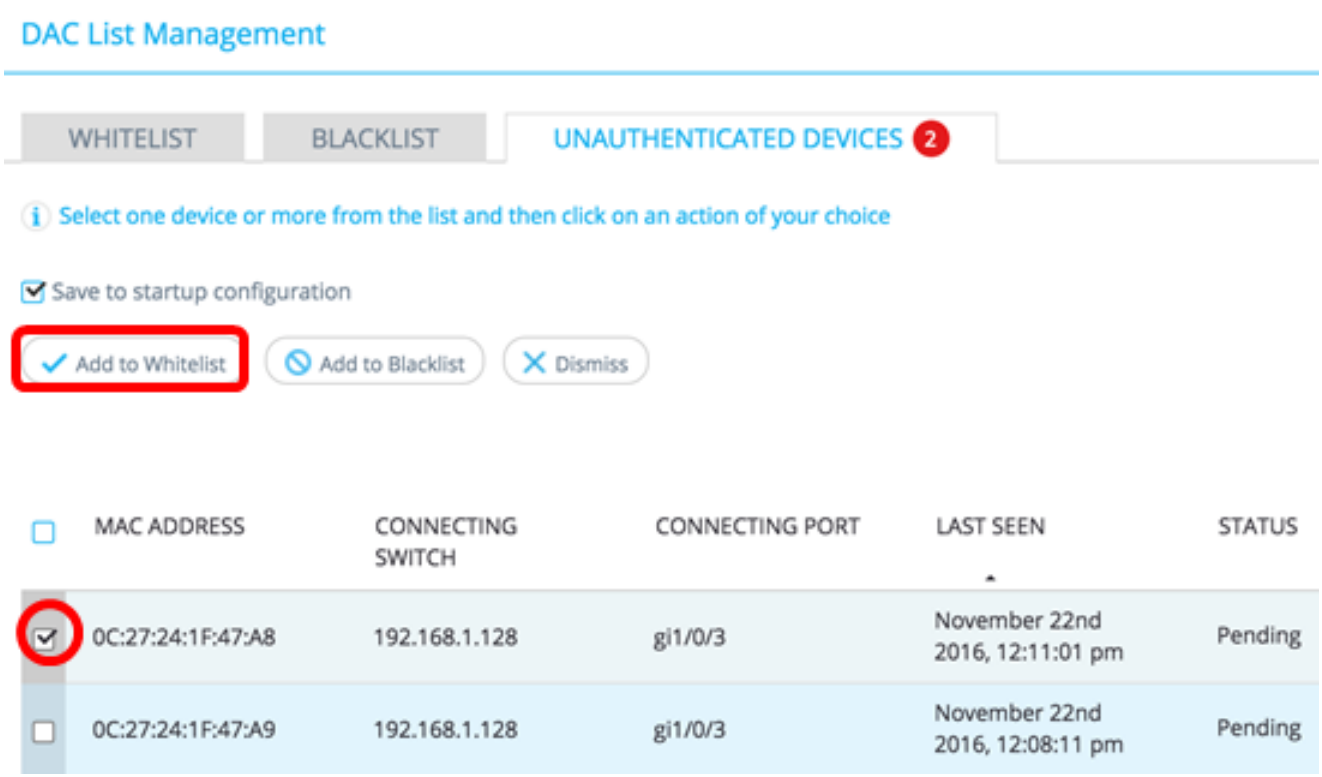


Passaggio 3. Fare clic sulla scheda **UNAUTHENTICATED DEVICES**. In questa pagina viene visualizzato l'elenco di tutte le periferiche non autenticate.

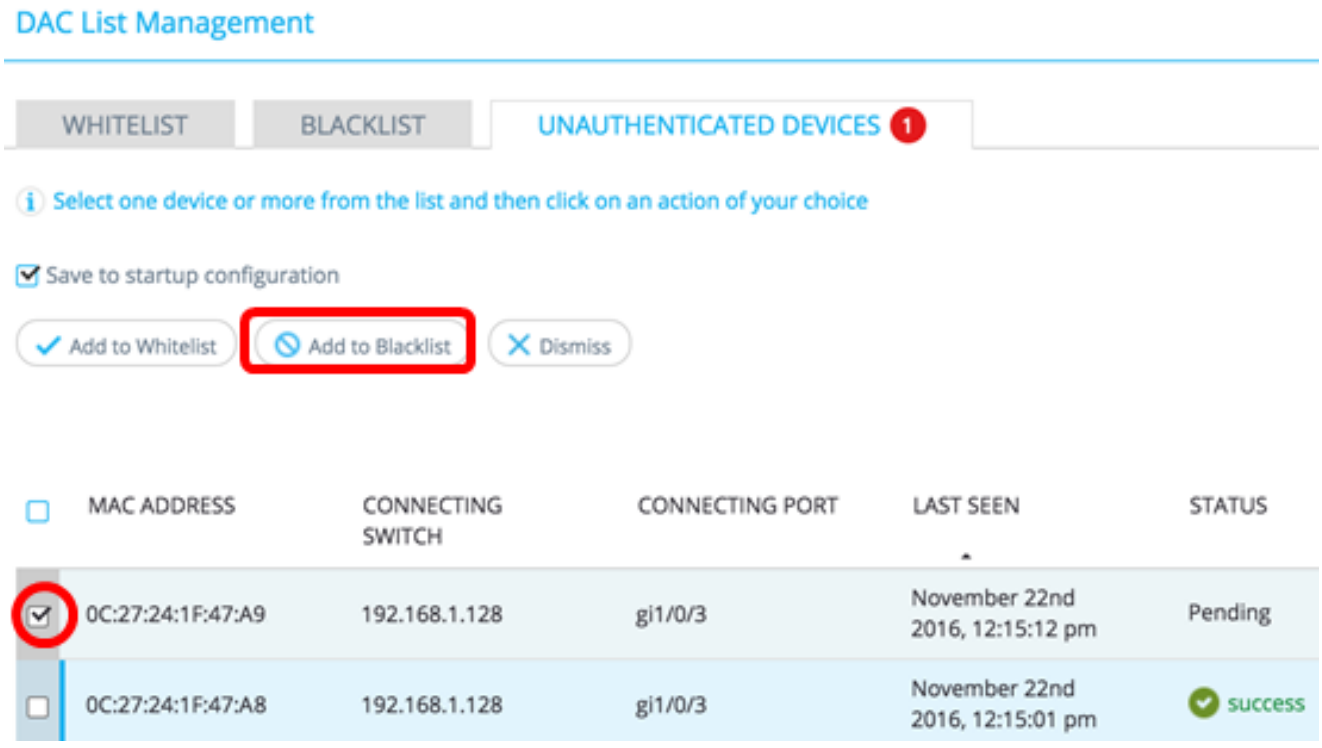


Nota: In alternativa, è possibile fare clic sull'icona DAC List Management System nell'angolo superiore destro della pagina SNA.

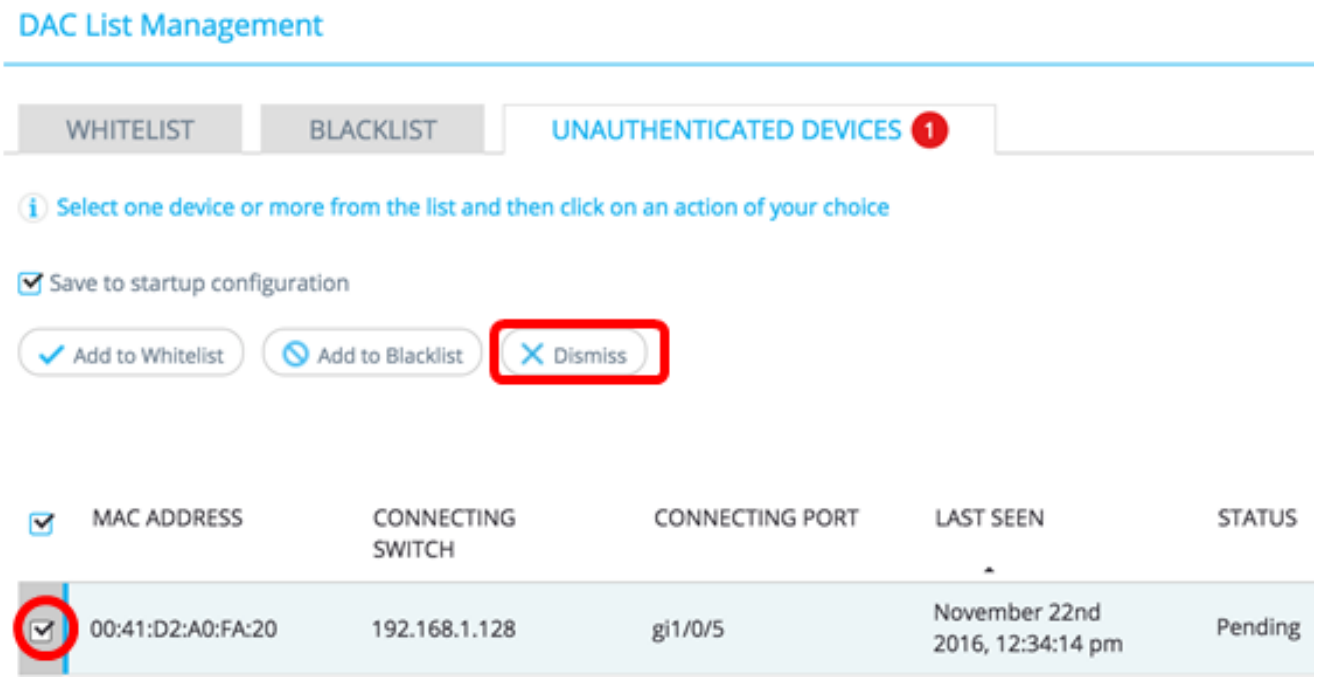
Passaggio 4. (Facoltativo) Selezionare la casella di controllo accanto all'indirizzo MAC del dispositivo o dei dispositivi che si desidera aggiungere all'elenco dei dispositivi consentiti e fare clic su **Aggiungi all'elenco dei dispositivi consentiti**.



Passaggio 5. (Facoltativo) Selezionare la casella di controllo accanto all'indirizzo MAC del dispositivo o dei dispositivi che si desidera aggiungere all'elenco di blocco e fare clic su **Aggiungi all'elenco di blocco**.



Passaggio 6. (Facoltativo) Selezionare la casella di controllo accanto all'indirizzo MAC del dispositivo o dei dispositivi che si desidera eliminare e fare clic su **Ignora**.

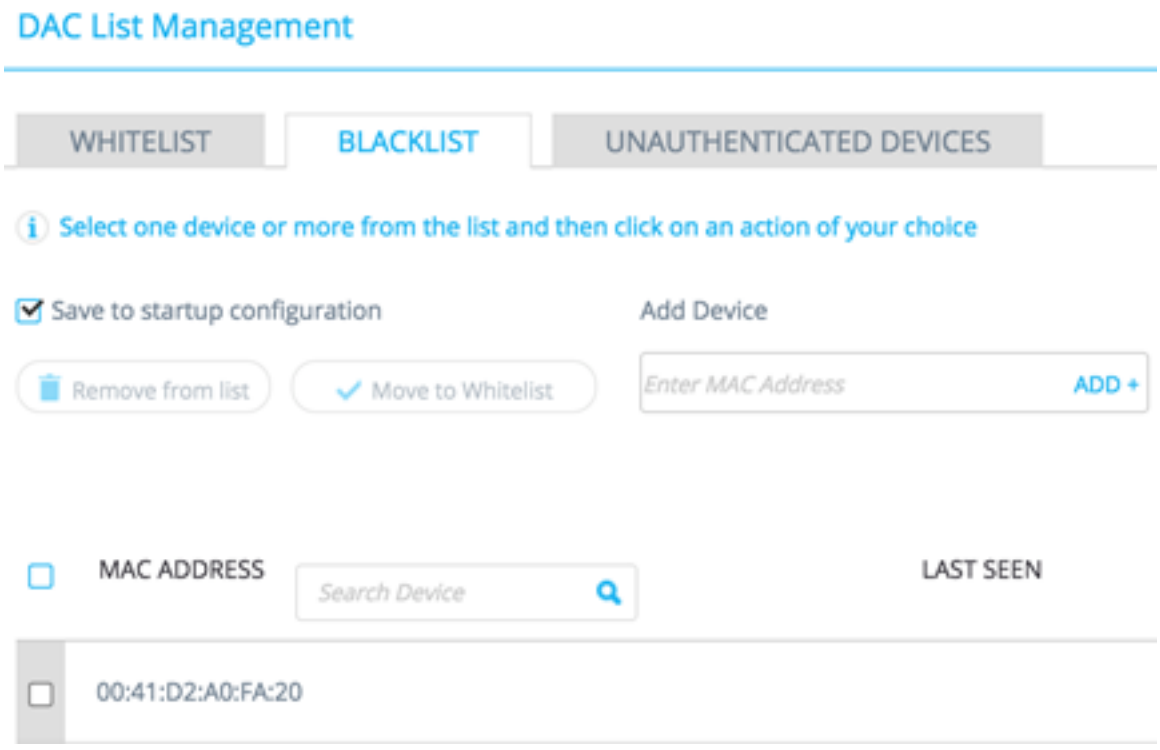


Nota: Tutti i pacchetti in entrata sulle porte del dispositivo vengono autenticati sul server RADIUS.

A questo punto è necessario aggiungere un dispositivo all'elenco dei dispositivi consentiti o bloccati.

Gestisci dispositivi nell'elenco Consenti o Blocca

Per gestire gli elenchi Consenti o Blocca, fare clic sulla scheda **ELENCO CONSENTI** o **ELENCO BLOCCA**.



In queste pagine è possibile eseguire i task riportati di seguito.

- Rimuovi dall'elenco — questa azione rimuove il dispositivo o i dispositivi selezionati dall'elenco.

- Sposta nell'elenco Blocca o Sposta nell'elenco Consenti — questa azione sposta il dispositivo o i dispositivi selezionati nell'elenco specificato.
- Aggiungi un dispositivo — questa azione aggiunge un dispositivo all'elenco Blocca o Consenti immettendo il relativo indirizzo MAC e facendo clic sul pulsante **AGGIUNGI+**.
- Cerca un dispositivo utilizzando l'indirizzo MAC — Inserisci un indirizzo MAC e fai clic sul **Cerca** pulsante.

A questo punto, i dispositivi nell'elenco di applicazione livello dati dovrebbero essere gestiti.