Configurazione RADIUS sugli switch gestiti serie 200/300

Obiettivo

RADIUS (Remote Authorization Dial-In User Service) è un servizio di sicurezza utilizzato per l'autenticazione degli utenti nelle reti con architettura di sicurezza centralizzata. Gli switch gestiti serie 200/300 possono fungere da client RADIUS nella rete e, insieme a un server RADIUS, è possibile stabilire un sistema centralizzato per l'autenticazione degli utenti nella rete. In questo documento viene spiegato come configurare un server RADIUS e applicare i metodi di autenticazione sugli switch gestiti serie 200/300.

Dispositivi interessati | Versione software

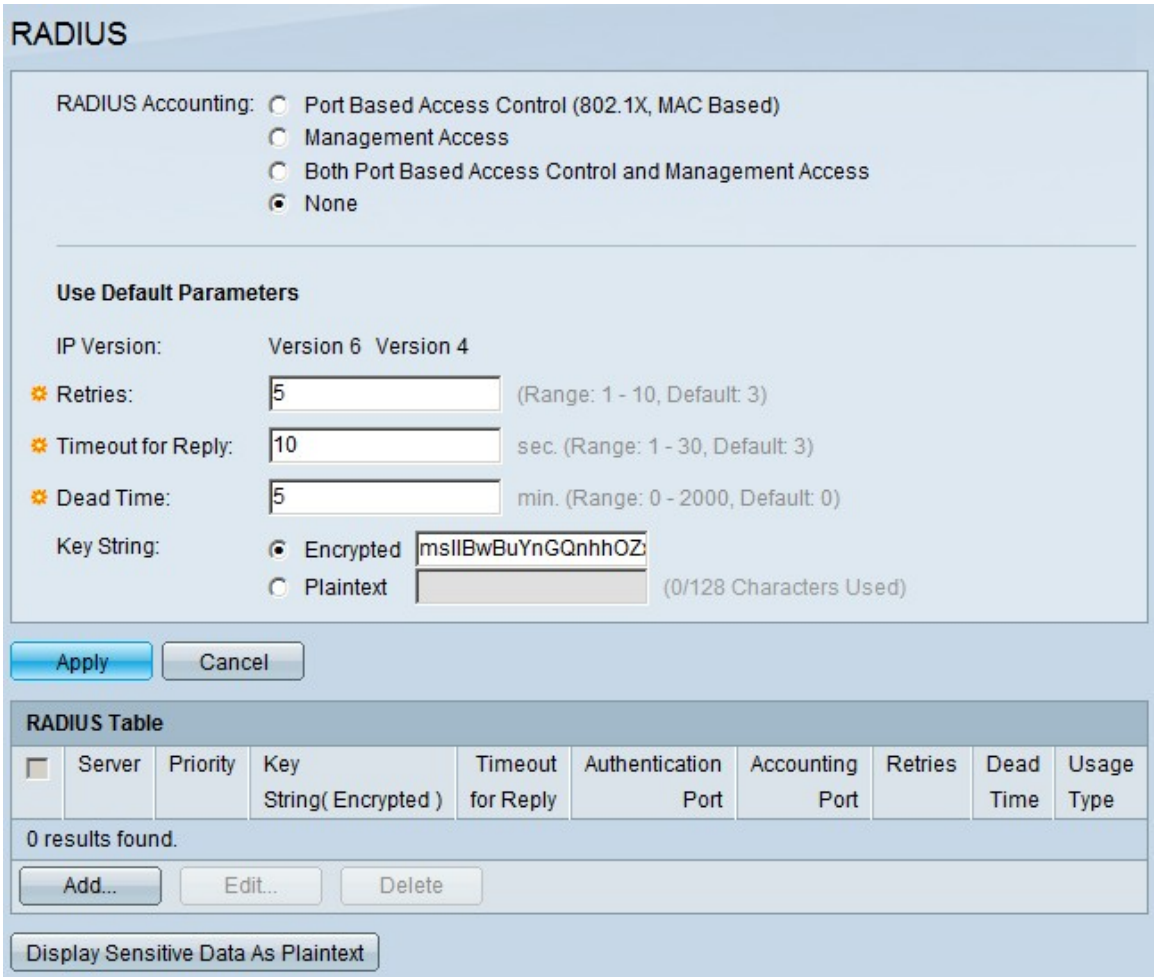
- SF/SG serie 200 - 1.2.9.x
- SF/SG serie 300 - 1.2.9.x

Configurazione predefinita RADIUS

In questa sezione viene illustrata la configurazione predefinita di un server RADIUS. Questi valori predefiniti possono essere utilizzati per qualsiasi server RADIUS che si desidera aggiungere a uno switch.

Passaggio 1

Accedere all'utility di configurazione Web e scegliere **Sicurezza > RADIUS**. Viene visualizzata la pagina *RADIUS*:



Le immagini di questo articolo fanno riferimento a uno switch modello SG300.

Passaggio 2

Nel campo Accounting RADIUS fare clic su una delle opzioni seguenti:

- Controllo degli accessi basato sulla porta (802.1x, basato sull'indirizzo MAC) - Consente di utilizzare il server RADIUS per l'accounting della porta 802.1x.
- Accesso di gestione - Per utilizzare il server RADIUS per l'accounting di accesso.
- Controllo degli accessi basato sulle porte e accesso alla gestione: per utilizzare il server RADIUS sia per l'accounting 802.1x che per l'account di accesso.
- Nessuno: per non utilizzare il server RADIUS per scopi di accounting.

Radius Accounting non è disponibile sugli switch serie SG200.

Passaggio 3

Nel campo Tentativi della sezione Usa parametri predefiniti immettere il numero di tentativi eseguiti dallo switch per autenticare il server RADIUS.

Passaggio 4

Nel campo Timeout per risposta immettere il tempo in secondi per ogni tentativo di autenticazione al server RADIUS.

Passaggio 5

Nel campo Dead Time (Tempo morto), immettere il tempo in minuti prima che lo switch dichiari un server RADIUS non reattivo come inattivo e passi al successivo server disponibile per tentare la connessione.

Passaggio 6

Nel campo Stringa chiave immettere la chiave utilizzata per l'autenticazione e la crittografia tra lo switch e il server RADIUS. La chiave deve corrispondere sia sul server RADIUS che sullo switch. Fare clic su una delle opzioni seguenti:

- Crittografata: se si dispone di una chiave crittografata da un altro dispositivo, immettere la chiave.
- Testo normale: se non si dispone di una chiave crittografata da un altro dispositivo, immettere la chiave come testo normale.

Passaggio 7

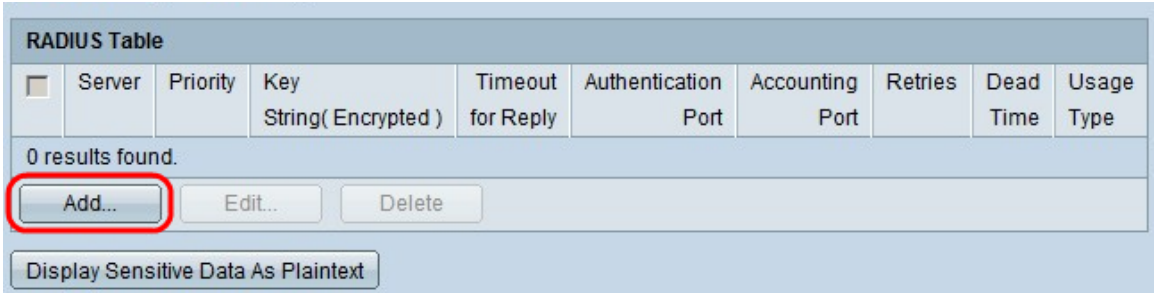
Fare clic su **Applica** per salvare i valori predefiniti e renderli disponibili per un server RADIUS.

Aggiunta/modifica di un server RADIUS

In questa sezione viene descritta una procedura dettagliata per aggiungere o modificare un server RADIUS a uno switch gestito serie 200/300.

Passaggio 1

Accedere all'utility di configurazione Web e scegliere **Sicurezza > RADIUS**. Viene visualizzata la pagina *RADIUS*:



Passaggio 2

Nella sezione Tabella RADIUS (RADIUS Table), fate clic su **Aggiungi (Add)**. Viene visualizzata la finestra *Aggiungi server Radius*.

Per modificare un server Radius corrente, fare clic su **Modifica** e modificare le proprietà desiderate del server RADIUS.

Passaggio 3

Nel campo Definizione server fare clic su una delle opzioni seguenti:

- Per nome: se il server RADIUS è definito con un nome.
- Per indirizzo IP: se il server RADIUS è definito con un indirizzo IP.

Passaggio 4

Nel campo Versione IP selezionare **Versione 6** o **Versione 4** come tipo di indirizzo IP del server RADIUS.

Passaggio 5

Se si sceglie **Versione 6** come indirizzo IP nel tipo di indirizzo IPv6, fare clic su una delle opzioni seguenti:

- Collegamento locale: indirizzo IPv6 che identifica solo gli host su un singolo collegamento di rete.
- Globale - Indirizzo IPv6 raggiungibile da altre reti.

Passaggio 6

Se come tipo di indirizzo IPv6 si sceglie Collega locale, nell'elenco a discesa Collega interfaccia locale selezionare l'interfaccia appropriata.

Passaggio 7

Nel campo Server IP Address/Name (Indirizzo IP/Nome server), immettere l'indirizzo IP o il nome del server RADIUS.

Passaggio 8

Nel campo Priority (Priorità), immettere la priorità del server RADIUS che lo switch utilizzerà. Il server con la priorità più alta viene interrogato per primo nello switch. Zero (0) indica la priorità più alta.

Passaggio 9

Nel campo Stringa chiave fare clic su una delle opzioni seguenti:

- Usa predefinito - Consente di utilizzare la chiave predefinita per l'autenticazione.
- Definita dall'utente (crittografata): se disponibile, immettere la chiave crittografata.
- Definito dall'utente (testo normale) - Se non è disponibile, immettere la chiave come testo normale.

Passaggio 10

Nel campo Timeout per risposta fare clic su una delle opzioni seguenti:

- Usa default (Use Default) - Consente di utilizzare il valore predefinito.

- Definito dall'utente: immettere il numero in secondi di attesa dello switch per ogni tentativo di connessione al server RADIUS.

Passaggio 11

Nel campo Porta di autenticazione, immettere la porta UDP utilizzata dal server RADIUS per l'autenticazione.

Passaggio 12

Nel campo Porta di accounting, immettere la porta UDP utilizzata dal server RADIUS per l'accounting.

Passaggio 13

Nel campo Tentativi fare clic su una delle opzioni seguenti:

- Usa default (Use Default) - Consente di utilizzare il valore predefinito.
- Definito dall'utente (User Defined) - Consente di utilizzare un valore diverso. Immettere il numero di tentativi che lo switch compie prima che la connessione al server RADIUS venga considerata interrotta.

Passaggio 14

Nel campo Tempo morto, fare clic su una delle seguenti opzioni:

- Usa default (Use Default) - Consente di utilizzare il valore predefinito.
- Definito dall'utente (User Defined) - Consente di utilizzare un valore diverso. Immettere, in minuti, il tempo che deve trascorrere prima che lo switch dichiari inattivo un server RADIUS che non risponde e passi al successivo server disponibile per tentare la connessione.

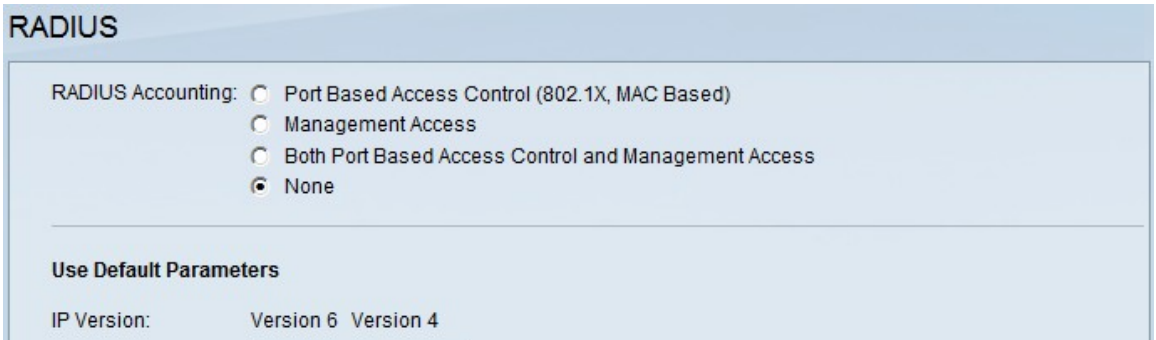
Passaggio 15

Nel campo Tipo di utilizzo fare clic su una delle opzioni seguenti:

- Login - Autentica gli amministratori dello switch.
- 802.1x - Il server RADIUS verificherà le credenziali di sicurezza degli utenti che richiedono l'accesso alla rete in base allo schema PNAC (Network Access Control) basato sulla porta 802.1x.
- All - Utilizza entrambi i tipi di autenticazione.

Passaggio 16

Fare clic su **Apply** (Applica).



Passaggio 17

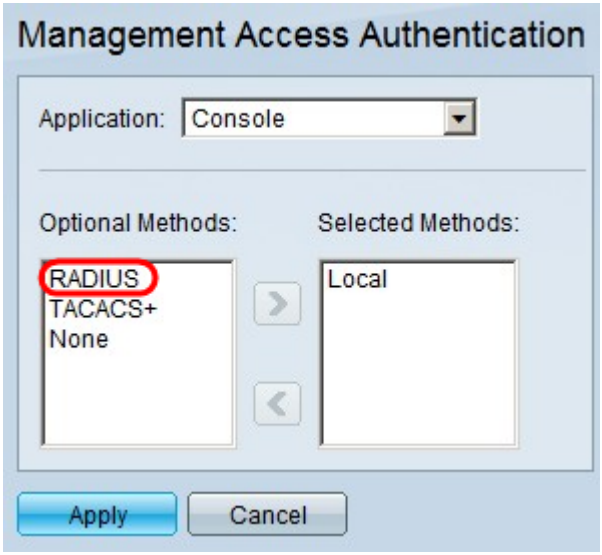
(Facoltativo) Per eliminare un server RADIUS, nella sezione Tabella RADIUS selezionare la casella di controllo del server RADIUS che si desidera eliminare e fare clic su **Elimina**.

Autenticazione RADIUS

Dopo aver configurato correttamente il server RADIUS, è necessario autenticarlo sullo switch. In questa sezione viene spiegato come autenticare un server RADIUS sugli switch gestiti serie 200/300.

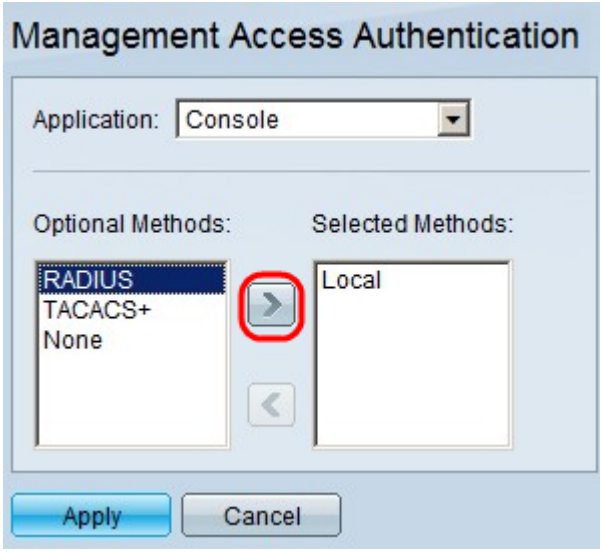
Passaggio 1

Accedere all'utility di configurazione Web e scegliere **Sicurezza > Autenticazione di accesso alla gestione**. Viene visualizzata la pagina *Management Access Authentication* (Autenticazione accesso gestione).



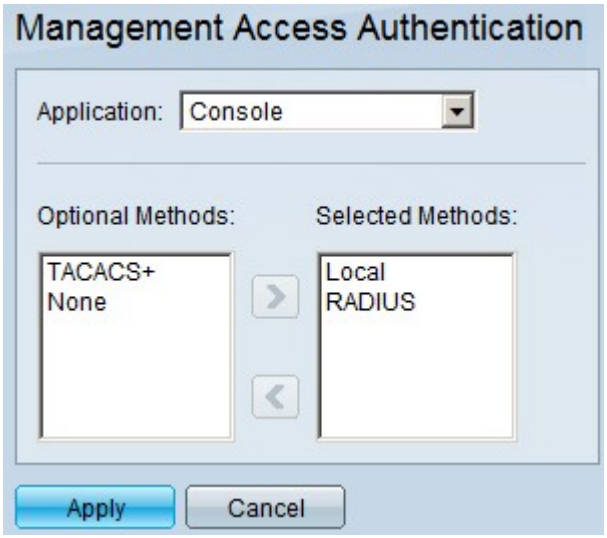
Passaggio 2

Nell'elenco Metodi facoltativi scegliere RADIUS.



Passaggio 3

Fare clic sul pulsante **>**.



Passaggio 4

Fare clic su **Apply** (Applica).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).