Autenticazione dell'accesso alla gestione sugli switch gestiti serie 200/300

Obiettivo

Le modalità di accesso alla gestione, come SSH, Console, Telnet, HTTP e HTTPS, consentono a un utente di accedere a un dispositivo. L'autenticazione può essere richiesta agli utenti per migliorare la sicurezza. Gli switch gestiti serie 200 e 300 possono essere autenticati localmente o su un server TACACS+ o RADIUS. Questo documento spiega come assegnare un metodo di autenticazione sugli switch gestiti serie 200 e 300.

Dispositivi interessati

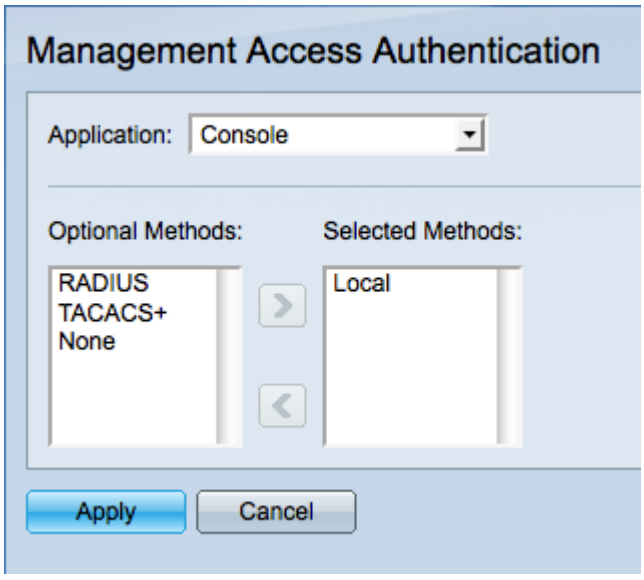
·SF/SG serie 200 e SF/SG serie 300 Managed Switch

Versione del software

•1.3.0.62

Autenticazione dell'accesso alla gestione

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. Selezionare il tipo di applicazione a cui si desidera assegnare l'autenticazione dall'elenco a discesa Applicazione. Le applicazioni possibili sono:

·Console: consente di gestire lo switch con un'interfaccia console. Permette di connettersi allo switch e di eseguire alcune configurazioni anche se l'indirizzo IP dello switch non è noto.

·Telnet: protocollo di comunicazione basato su caratteri che consente di connettersi in remoto allo switch tramite una rete TCP/IP. Telnet non è consigliato a causa della

mancanza di crittografia.

·SSH (Secure Telnet): esegue le stesse funzioni della crittografia Telnet Plus. SSH è consigliato per le connessioni remote.

·HTTP: protocollo che consente di accedere all'interfaccia utente grafica (GUI) dello switch. a differenza delle configurazioni Telnet e SSH, che sono basate sul prompt dei comandi.

·HTTP protetto (HTTPS): esegue le stesse funzioni di HTTP con l'aggiunta di comunicazioni protette.

Passaggio 3. Scegliere un metodo di autenticazione dall'elenco Metodi facoltativi, quindi fare clic sul pulsante **>** per spostarlo nell'elenco Metodi selezionati. Metodi diversi forniscono diversi livelli di protezione.

Nota: l'ordine in cui vengono selezionati i metodi di autenticazione corrisponde all'ordine in cui viene eseguita l'autenticazione utente. Se si seleziona RADIUS prima di quello locale, il dispositivo tenterà di autenticare l'utente tramite un server RADIUS prima del metodo locale.

·RADIUS: RADIUS esegue la crittografia solo della password. L'autenticazione viene eseguita su un server RADIUS e richiede un server RADIUS configurato.

·TACACS+: TACACS+ crittografa tutti i dati durante l'autenticazione. L'autenticazione viene effettuata su un server TACACS+ e richiede un server TACACS+ configurato.

·Nessuno: per accedere allo switch non è necessaria l'autenticazione.

·Locale: le informazioni sull'utente vengono verificate dalle informazioni memorizzate sullo switch.

Passaggio 4. Fare clic su **Applica** per salvare le impostazioni di autenticazione oppure su **Annulla** per annullare le modifiche.

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).