

# Configurazione delle regole del profilo di accesso sugli switch gestiti serie 200/300

## Obiettivi

Il profilo di accesso funge da altro livello di protezione per lo switch. I profili di accesso possono contenere fino a 128 regole per aumentare la protezione. Ogni regola contiene un'azione e un criterio. Se il metodo di accesso non corrisponde al metodo di gestione, l'utente viene bloccato e non può accedere allo switch.

In questo documento viene spiegato come configurare le regole di profilo sugli switch gestiti serie 200/300.

## Dispositivi interessati

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

## Versione del software

·v1.2.7.76

## Configurazione profili di accesso

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza > Metodo di accesso alla gestione > Regole profilo**. Viene visualizzata la pagina *Regole profili*:

<input checked="" type="checkbox"/>	Access Profile Name	Priority	Management Method	Action	Interface	Source IP Address	Prefix Length
<input checked="" type="checkbox"/>	Guest	1	Secure HTTP (SSL)	Permit	FE3	192.168.10.0	24
<input type="checkbox"/>	Console Only	1	All	Deny			

Passaggio 2. Selezionare la casella di controllo **Filtro** per visualizzare il nome del profilo di accesso creato nella pagina *Profilo di accesso*.

Passaggio 3. Selezionare il profilo di accesso desiderato dall'elenco a discesa Nome profilo di accesso uguale a.

Passaggio 4. Fare clic su **Go** per visualizzare il profilo di accesso desiderato.

Passaggio 5. (Facoltativo) Per avviare una nuova ricerca, fare clic su **Cancella filtro**.

## Aggiungi regola di profilo

Passaggio 1. Selezionare la casella di controllo corrispondente al profilo di accesso a cui si

desidera aggiungere una regola.

Passaggio 2. Fare clic su **Add**. Viene visualizzata la finestra *Aggiungi regola profilo*.

Access Profile Name: Guest

Rule Priority: 2 (Range: 1 - 65535)

Management Method:

- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)
- SNMP

Action:

- Permit
- Deny

Applies to Interface:  All  User Defined

Interface:  Port FE4  LAG 1  VLAN 1

Applies to Source IP Address:  All  User Defined

IP Version:  Version 6  Version 4

IP Address: 192.168.20.0

Mask:

- Network Mask
- Prefix Length 24 (Range: 0 - 32)

Apply Close

Passaggio 3. (Facoltativo) Per aggiungere una regola di profilo a un nome di profilo diverso, scegliere il nome del profilo desiderato dall'elenco a discesa Nome profilo di accesso.

Passaggio 4. Immettere la priorità della regola nel campo Priorità regola. La priorità della regola corrisponde ai pacchetti con le regole. Le regole con priorità inferiore vengono controllate per prime. Se un pacchetto soddisfa una regola, viene eseguita l'azione desiderata.

Passaggio 5. Fare clic sul pulsante di opzione corrispondente al metodo di gestione desiderato nel campo Metodo di gestione. Il metodo di accesso utilizzato dall'utente deve corrispondere al metodo di gestione per l'azione da eseguire.

- Tutti - Tutti i metodi di gestione vengono assegnati al profilo di accesso.
- Telnet: il metodo di gestione Telnet viene assegnato alla regola. Solo gli utenti con un metodo di profilo di accesso riunione Telnet possono accedere al dispositivo.
- SSH (Secure Telnet): il metodo di gestione SSH è assegnato al profilo. Solo gli utenti con un profilo di accesso riunione Telnet protetto possono accedere al dispositivo.
- HTTP: il metodo di gestione HTTP viene assegnato al profilo. Solo gli utenti con il metodo di profilo di accesso alla riunione HTTP possono accedere al dispositivo.

- HTTP protetto (SSL): il metodo di gestione HTTPS viene assegnato al profilo. Solo gli utenti con il metodo di profilo di accesso alla riunione HTTPS possono accedere al dispositivo.

- SNMP: il metodo di gestione SNMP viene assegnato al profilo. Gli utenti che dispongono solo del metodo di accesso alle riunioni SNMP possono accedere al dispositivo.

Passaggio 6. Scegliere l'azione da allegare alla regola dai pulsanti di opzione Azione. I valori possibili per l'azione sono:

- Permit (Autorizzazione): l'accesso allo switch è consentito.

- Nega: accesso negato allo switch.

Passaggio 7. Fare clic sul pulsante di scelta desiderato corrispondente al tipo di interfaccia desiderato nel campo Si applica all'interfaccia per definire l'interfaccia per il profilo di accesso.

- All: include tutte le interfacce, ad esempio porte, VLAN e LAG.

**Nota:** i LAG sono collegamenti logici che combinano più collegamenti fisici per fornire una maggiore larghezza di banda.

- Definito dall'utente - Si applica solo all'interfaccia desiderata per l'utente.

- Port: selezionare la porta dall'elenco a discesa Port per la quale definire il profilo di accesso.

- LAG - Selezionare il LAG dall'elenco a discesa LAG per il quale definire il profilo di accesso dall'elenco a discesa LAG.

- VLAN: selezionare la VLAN dall'elenco a discesa VLAN per cui definire il profilo di accesso dall'elenco a discesa VLAN.

Passaggio 8. Fare clic sul pulsante di opzione **Source IP Address** per abilitare l'indirizzo IP di origine dell'interfaccia. Sono disponibili due valori:

- Tutti: include tutti gli indirizzi IP.

- Definito dall'utente: si applica solo all'indirizzo IP desiderato per l'utente.

- Versione 6 — Per indirizzi IP versione 6.

- Versione 4 — Per indirizzi IP versione 4.

Passaggio 9. Se nel passaggio 7 è stata scelta l'opzione Definito dall'utente, immettere l'indirizzo IP del dispositivo nel campo Indirizzo IP.

Passaggio 10. Fare clic su un pulsante di scelta nel campo Maschera di una delle opzioni per definire la maschera di rete. Le opzioni disponibili sono:

- Network Mask: consente di immettere la subnet mask che corrisponde all'indirizzo IP nel formato decimale con punti.

- Lunghezza prefisso — immettere la lunghezza del prefisso della subnet mask che corrisponde all'indirizzo IP.

Passaggio 11. Fare clic su **Apply** (Applica).

**Profile Rules**

Profile Rule Table

Filter:  Access Profile Name equals to

<input type="checkbox"/>	Access Profile Name	Priority	Management Method	Action	Interface	Source IP Address	Prefix Length
<input type="checkbox"/>	Guest	1	Secure HTTP (SSL)	Permit	FE3	192.168.10.0	24
<input checked="" type="checkbox"/>	Guest	2	Secure Telnet (SSH)	Permit	FE4	192.168.20.0	24
<input type="checkbox"/>	Console Only	1	All	Deny			

Passaggio 12. (Facoltativo) Per modificare un profilo di accesso corrente, selezionare la casella di controllo del nome del profilo di accesso che si desidera modificare e fare clic su **Modifica**.

Passaggio 13. (Facoltativo) Per eliminare un profilo di accesso, selezionare la casella di controllo del profilo di accesso che si desidera eliminare e fare clic su **Elimina**.

## 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).