Creazione e gestione di regole SSD (Secure Sensitive Data) sugli switch gestiti serie 200/300

Obiettivo

In questo documento viene spiegato come configurare e gestire le regole per Secure Sensitive Data (SSD) sugli switch serie 200/300.

Dispositivi interessati

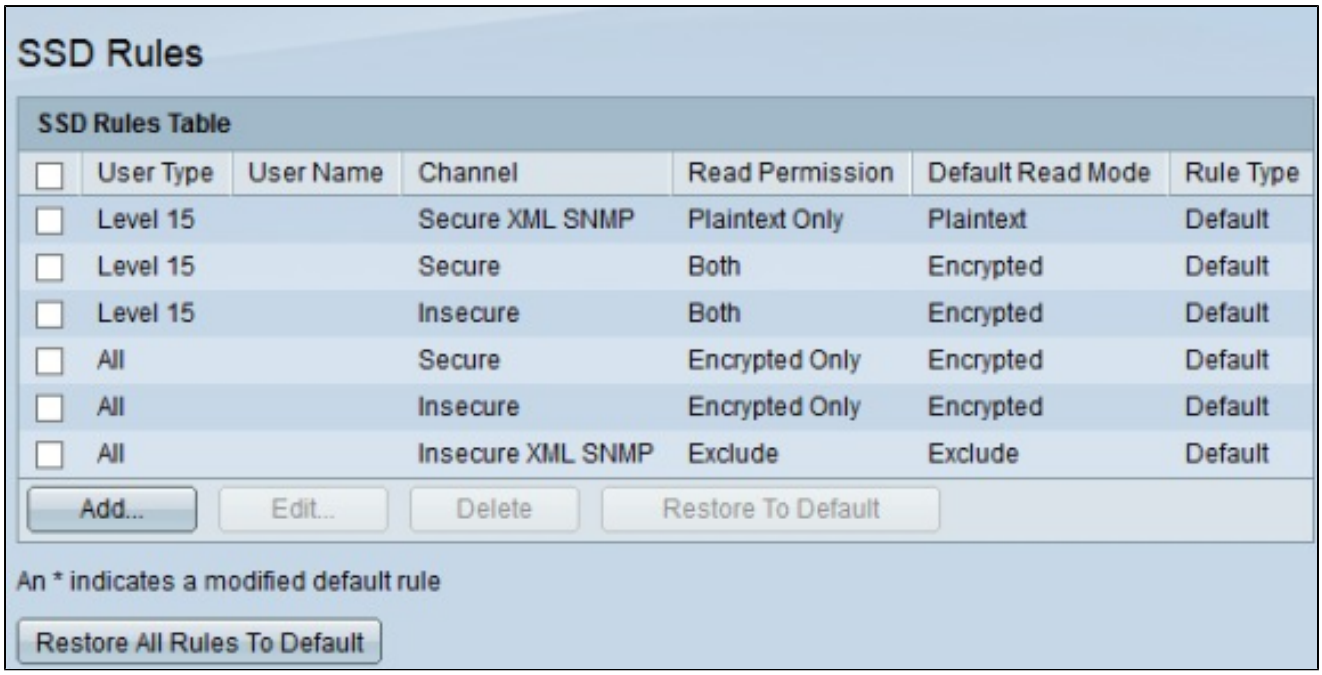
· SF/SG serie 200 e SF/SG serie 300 Managed Switch

Versione del software

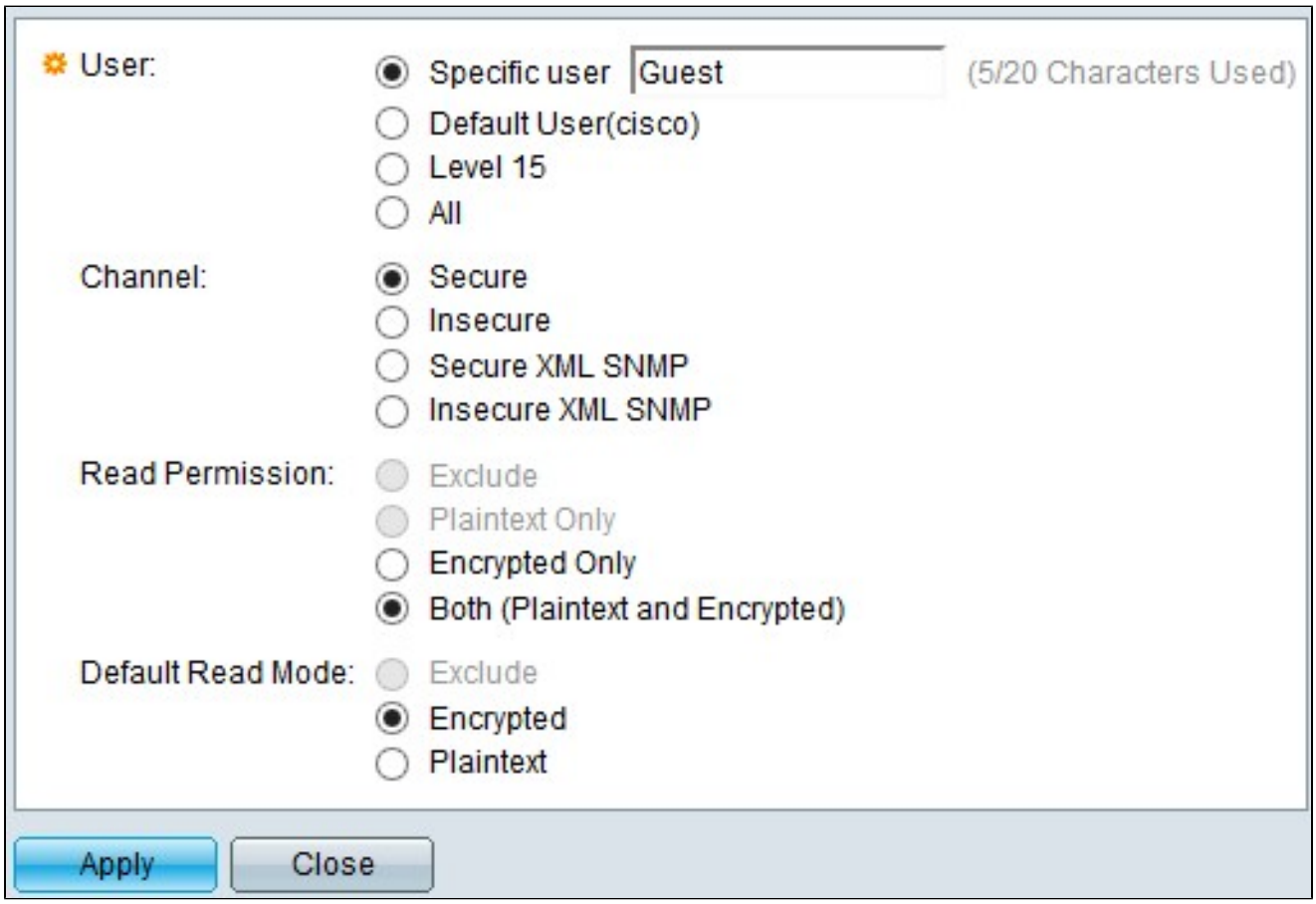
· v1.2.7.76

Regole SSD

Passaggio 1. Accedere all'utility di configurazione Web e scegliere Sicurezza > Gestione sicura dei dati sensibili > Regole SSD. Viene visualizzata la pagina Regole SSD.



Passaggio 2. Per creare una nuova regola, fare clic su Aggiungi. Verrà visualizzata la pagina Definizione regola.



Passaggio 3. Nel campo Utente, selezionare un pulsante di opzione per scegliere gli utenti a cui applicare la regola.

· Utente specifico - Immettere il nome utente specifico nel campo se la regola si applica a un singolo utente.

· Utente predefinito —. Questa regola si applica all'utente predefinito, impostato su cisco.

· Livello 15: questa regola si applica a tutti gli utenti con privilegi di livello 15.

· Tutti - Questa regola si applica a tutti gli utenti.

Passaggio 4. Nel campo Canale, scegliere un pulsante di opzione per determinare a quali canali applicare la regola.

· Protetto: questa regola viene applicata solo ai canali protetti. Sono inclusi la console, SSH e HTTPS, ma non i canali XML.

· Non protetto: questa regola viene applicata solo ai canali non protetti. Sono inclusi Telnet, TFTP e HTTP, ma non i canali XML.

· Secure XML SNMP: applica questa regola solo a XML su HTTPS con privacy.

· SNMP XML non sicuro: applica questa regola solo a XML su HTTP o senza privacy.

Passaggio 5. Nel campo Autorizzazione lettura, selezionare un pulsante di opzione in base alle selezioni precedenti.

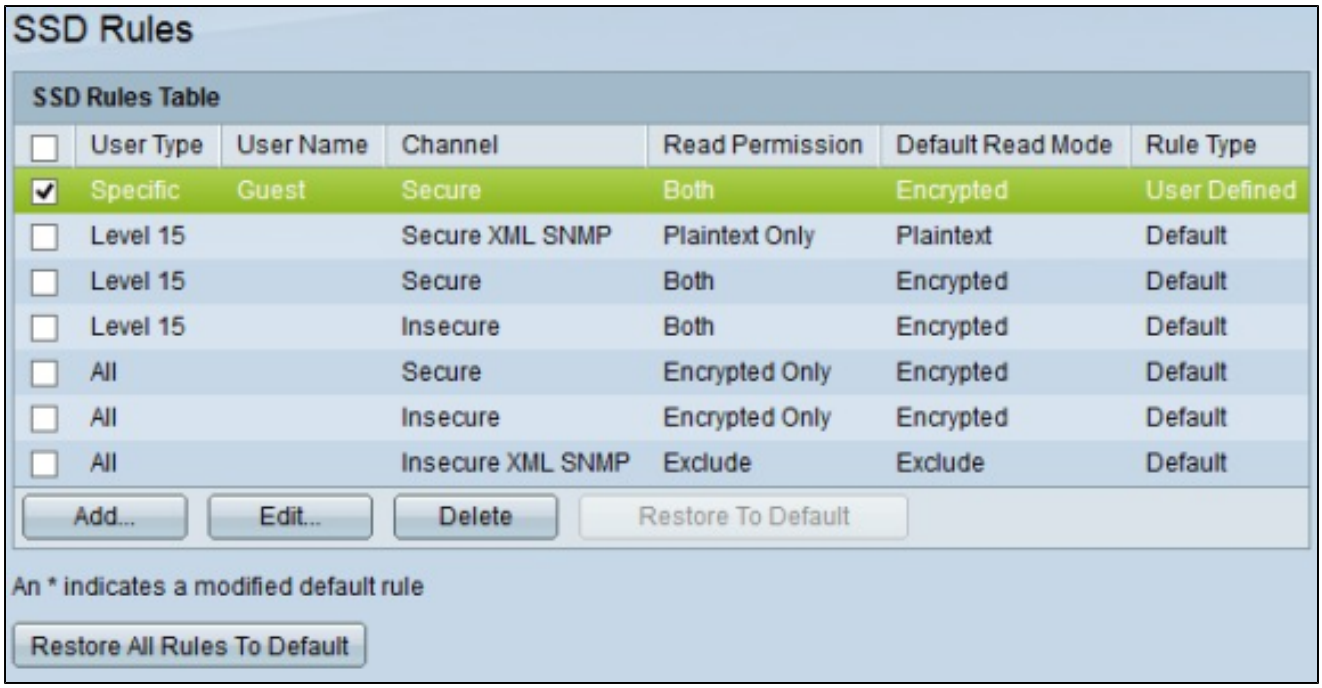
· Se nel passaggio 3 è stato scelto Livello 15 o Tutto, fare clic su Escludi o Solo testo normale.

· Se nel passaggio 4 è stato scelto SNMP XML protetto o SNMP XML non protetto, fare clic su Escludi o Solo testo normale.

· Se al punto 4 è stato scelto Protetto o Non protetto, fare clic su Solo crittografato o Entrambi (Testo normale e Crittografato).

Passaggio 6. Nel campo Modalità di lettura predefinita fare clic su Escludi, Crittografato o Testo normale.

Passaggio 7. Per attivare la regola, fare clic su Applica. Per annullare la creazione della regola, scegliere Chiudi.


SSD Rules
SSD Rules Table
User Type
User Name
Channel
Read Permission
Default Read Mode
Rule Type
Specific
Guest
Secure
Both
Encrypted
User Defined
Level 15
Secure XML SNMP
Plaintext Only
Plaintext
Default
Level 15
Secure
Both
Encrypted
Default
Level 15
Insecure
Both
Encrypted
Default
All
Secure
Encrypted Only
Encrypted
Default
All
Insecure
Encrypted Only
Encrypted
Default
All
Insecure XML SNMP
Exclude
Exclude
Default
Add...
Edit...
Delete
Restore To Default
An * indicates a modified default rule
Restore All Rules To Default

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).