# Secure Sensitive Data (SSD) Rules Configuration on Sx500 Series Stackable Switches

## Objective

Secure Sensitive Data (SSD) Management is used to manage sensitive data such as passwords and keys securely on the switch, populate this data to other devices, and to secure auto-configuration. Access to view the sensitive data as plaintext or encrypted is provided based on the user-configured access level and the access method of the user. This article explains how to manage SSD rules on the Sx500 Series Stackable Switches.

**Note:** You may also want to know how to manage the SSD properties. For details refer to the article *Secure Sensitive Data (SSD) Properties on Sx500 Series Stackable Switches*.

## Applicable Devices

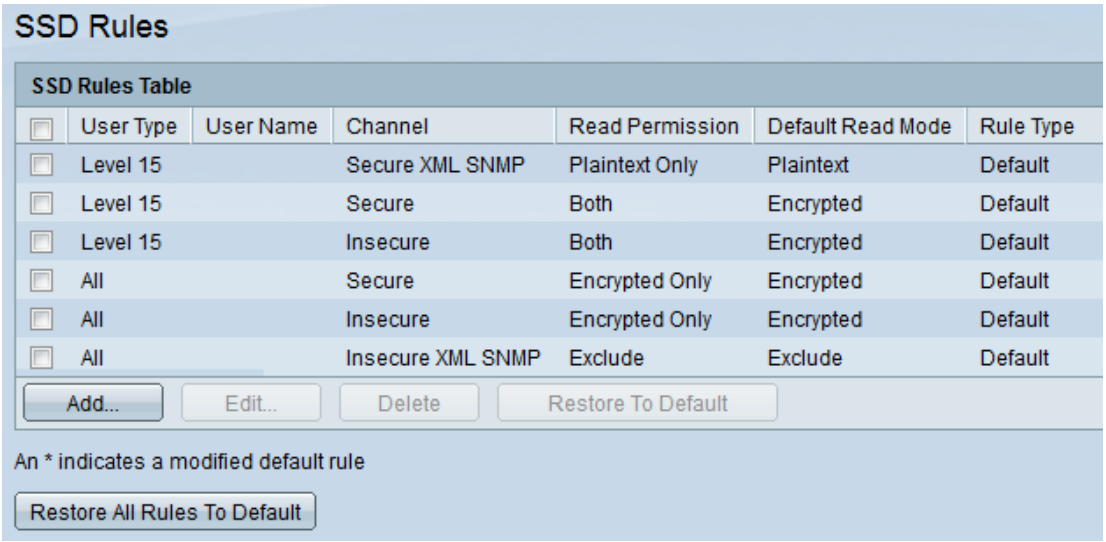
- Sx500 Series Stackable Switches

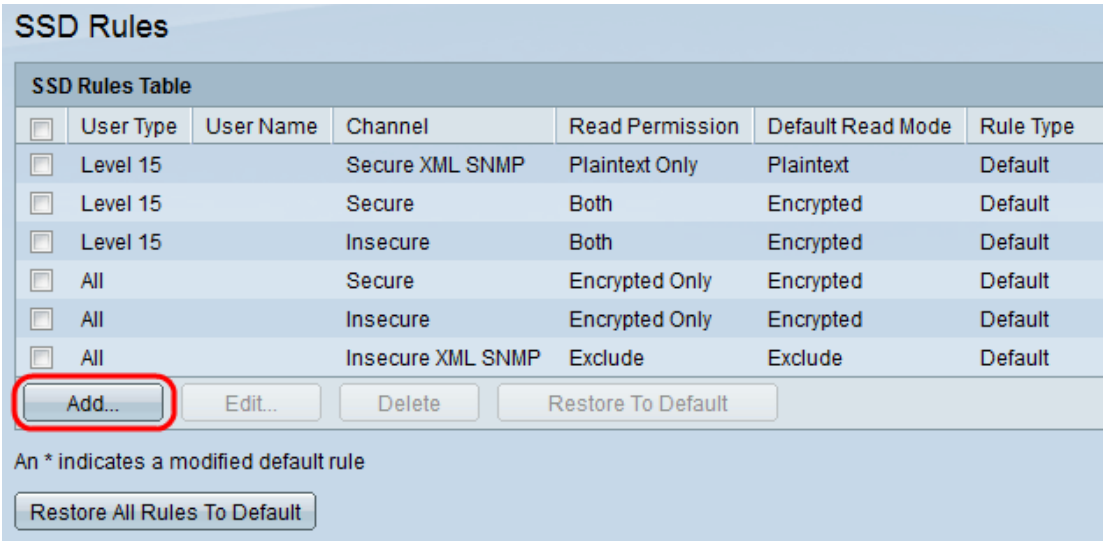
## Software Version

- v1.2.7.76

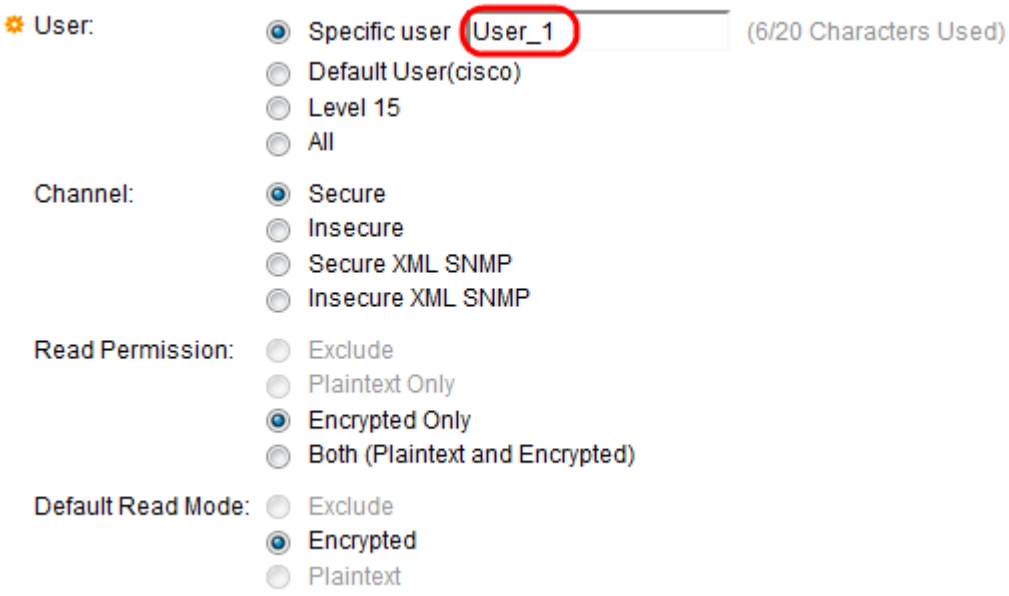
## SSD Rules Configuration

Step 1. Log in to the web configuration utility and choose **Security > Secure Sensitive Data Management > SSD Rules**. The *SSD Rules* page opens:



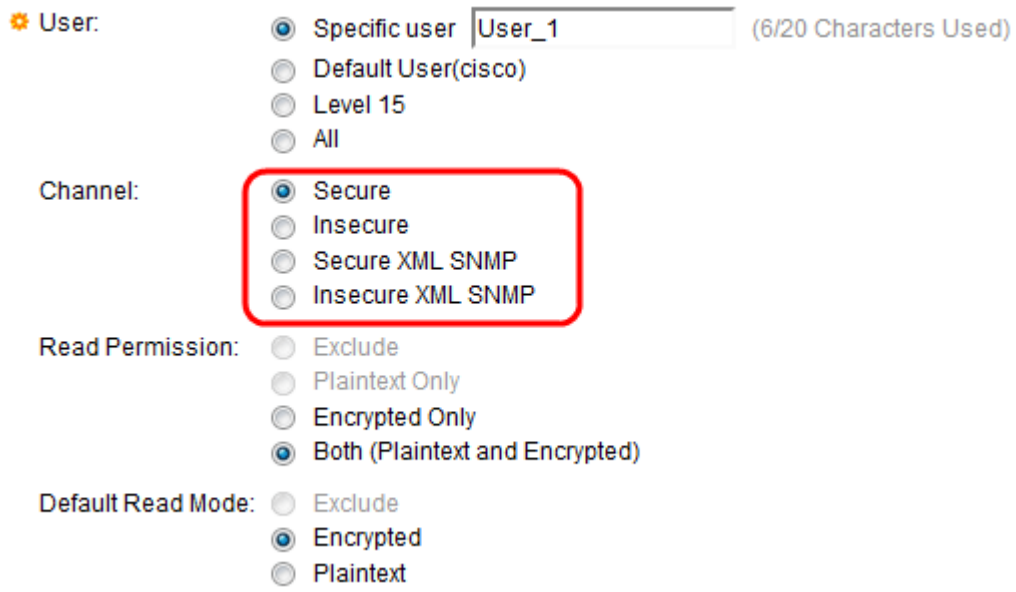



Step 2. Click **Add** to add a new SSD rule. The *Add SSD Rule* window appears.




Step 3. Click the desired User radio button to which the SSD rule appears. The available options are:

- Specific User — Enter the specific user name to which this rule applies (this user does not necessarily have to be defined).
- Default User (cisco) — The rule applies to the default user.
- Level 15 — The rule applies to all users with privilege level 15. Here the user can access the GUI and can configure the switch. To change the privilege settings refer to the article *User Account Configuration on Sx500 Series Stackable Switches*.
- All — The rule applies to all users.



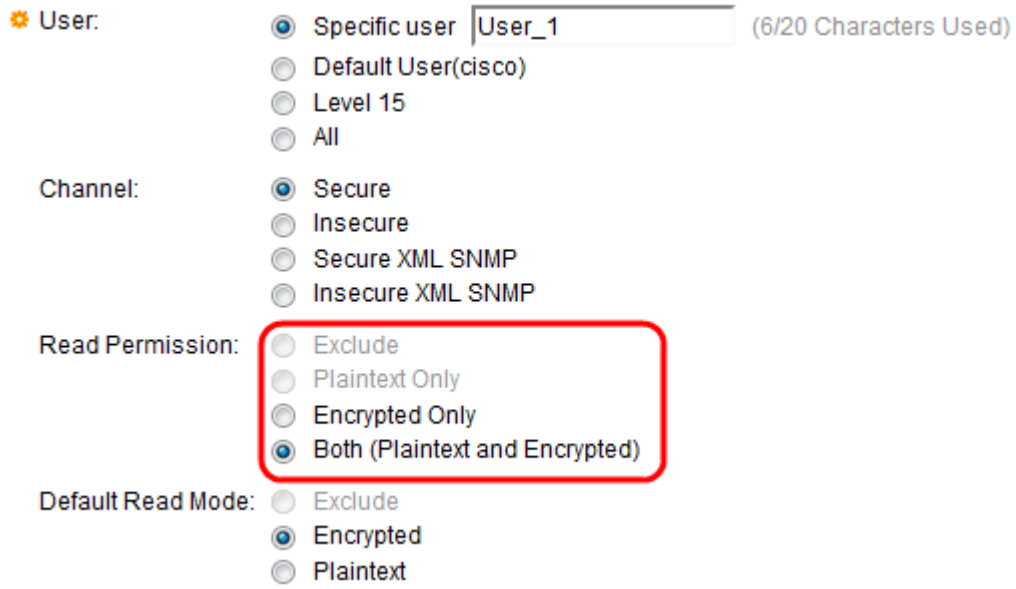

Step 4. Click the radio button that corresponds to the security level of the input channel to which the rule applies in the Channel field. The available options are:

• Secure — This rule applies only to secure channels (console, SCP, SSH, and HTTPS), not including the SNMP and XML channels.

• Insecure — This rule applies only to insecure channels (Telnet, TFTP, and HTTP), not including the SNMP and XML channels.

• Secure XML SNMP — This rule applies only to XML over HTTPS and SNMPv3 with privacy.

• Insecure XML SNMP — This rule applies only to XML over HTTP or SNMPv1/v2 and SNMPv3 without privacy.



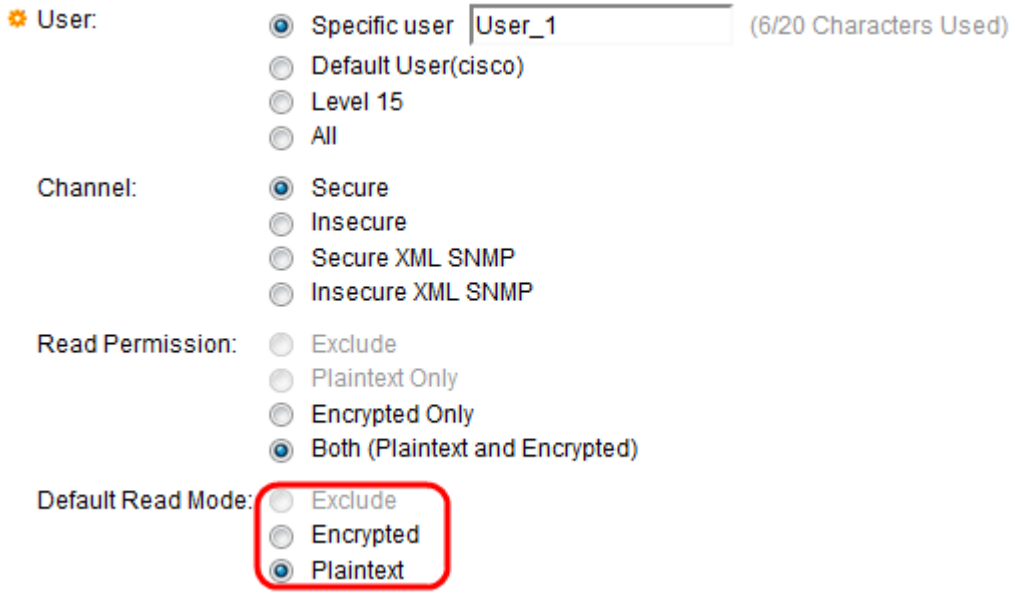

Step 5. Click the desired radio button to define the read permissions associated with the rule in the Read Permission field. The available options are:

• Exclude —The lowest level of read permission and the users are not allowed to receive sensitive data in any form. This option is available only if Insecure is clicked in Step 4.

• Plaintext Only — A higher level of read permission when compared to Exclude. This option allows the users to receive sensitive data in only plaintext format. This option is available only if Insecure is clicked in Step 4.

• Encrypted Only — The middle level of read permission. This option allows the users to receive sensitive data as encrypted only.

• Both (Plaintext and Encrypted) — The highest level of read permission. This option allows the users to receive both encrypted and plaintext permissions and is permitted to get sensitive data as encrypted and plaintext form.



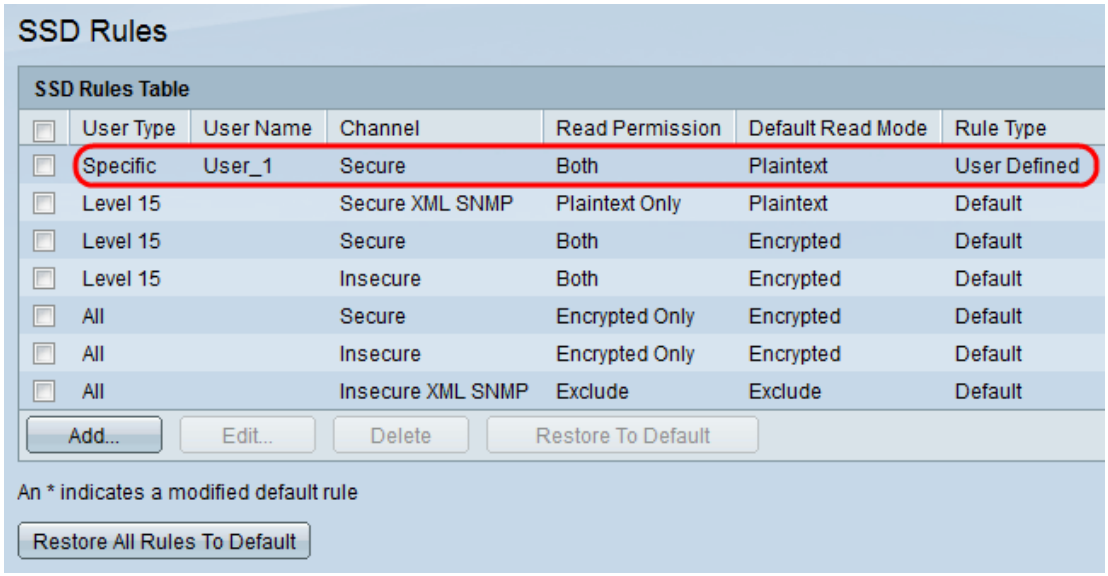

Step 6. Click the radio button that corresponds to the desired read mode from the Default Read Mode field. It defines the default permission given to all users. The Default Read Mode option does not have a higher priority than the Read Permission field. The available options are:

• Exclude — Does not allow you to read the sensitive data. This option is available only if Insecure is clicked in Step 4.

• Encrypted — Sensitive data is presented encrypted.

• Plaintext — Sensitive data is presented as plaintext.

Step 7. Click **Save** in the *Add SSD Rule* window. The changes are shown in the SSD Rules Table as shown below:


SSD Rules
SSD Rules Table
User Type
User Name
Channel
Read Permission
Default Read Mode
Rule Type
Specific
User_1
Secure
Both
Plaintext
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