Configuration sécurisée de règles des données sensibles (disque transistorisé) sur des commutateurs empilables de gamme Sx500

Objectif

La Gestion sécurisée des données sensibles (disque transistorisé) est utilisée pour gérer des données sensibles telles que des mots de passe et les clés sécurisé sur le commutateur, remplissent ces données à d'autres périphériques, et pour sécuriser la configuration automatique. Accédez à pour visualiser les données sensibles comme plaintext ou chiffré est fourni a basé sur le niveau d'accès utilisateur-configuré et la méthode d'accès de l'utilisateur. Cet article explique comment gérer des règles disque transistorisé sur les commutateurs empilables de gamme Sx500.

Remarque: Vous pouvez également vouloir savoir gérer les propriétés disque transistorisé. Pour des détails référez-vous aux *données sensibles sécurisées d'*article *(disque transistorisé) Properties sur des commutateurs empilables de gamme Sx500*.

Périphériques applicables

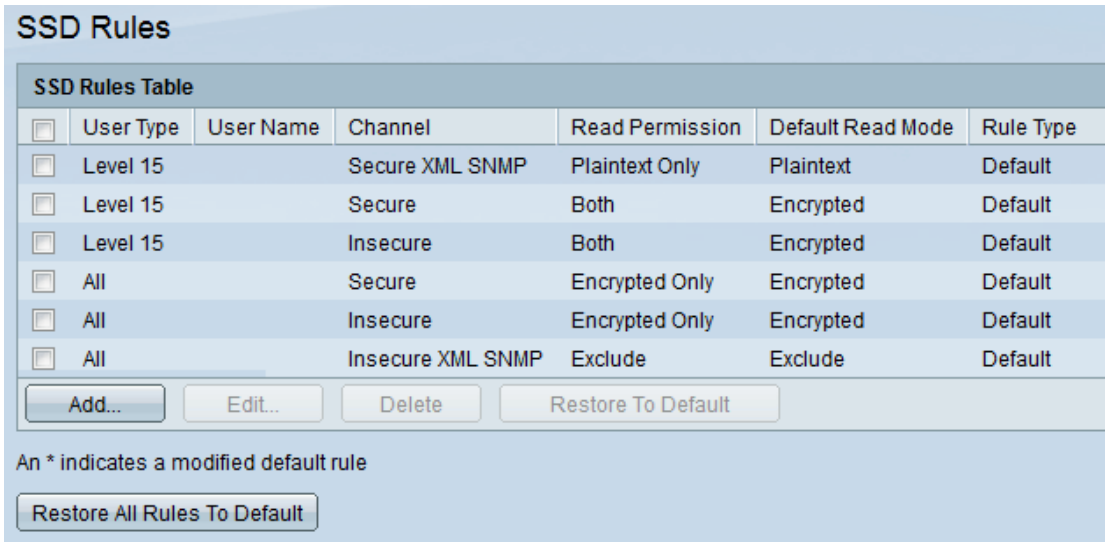
- Commutateurs empilables de gamme Sx500

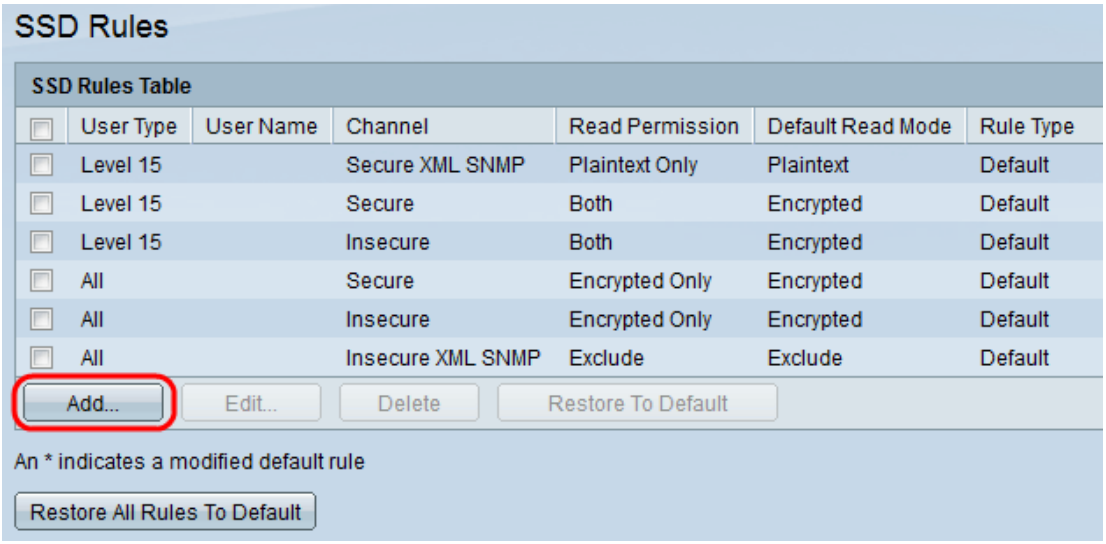
Version de logiciel

- v1.2.7.76

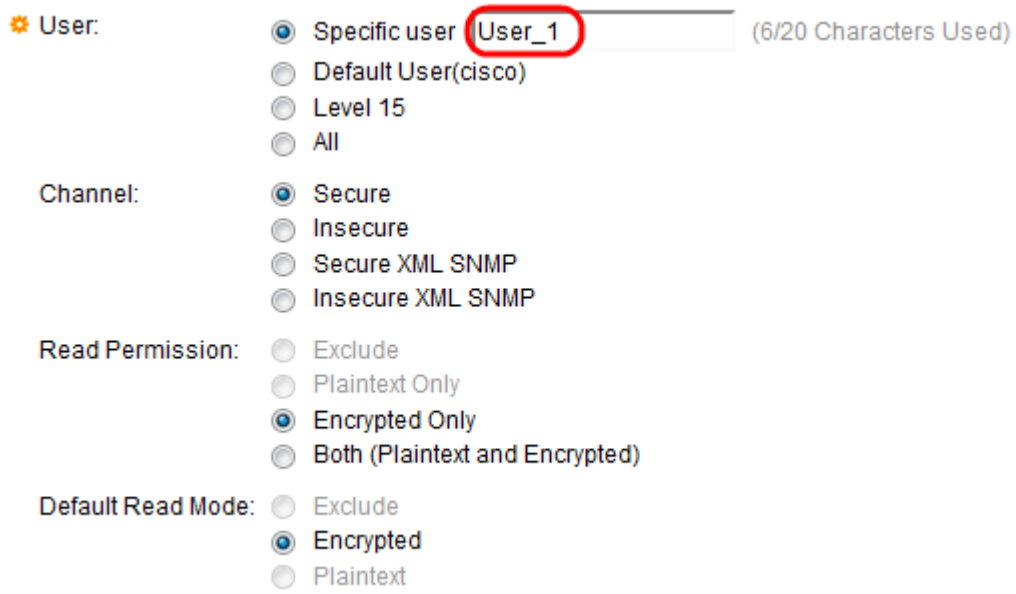
Le disque transistorisé ordonne la configuration

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **Sécurité > sécurisent la gestion de données sensible > les règles disque transistorisé**. La page de *règles disque transistorisé* s'ouvre :



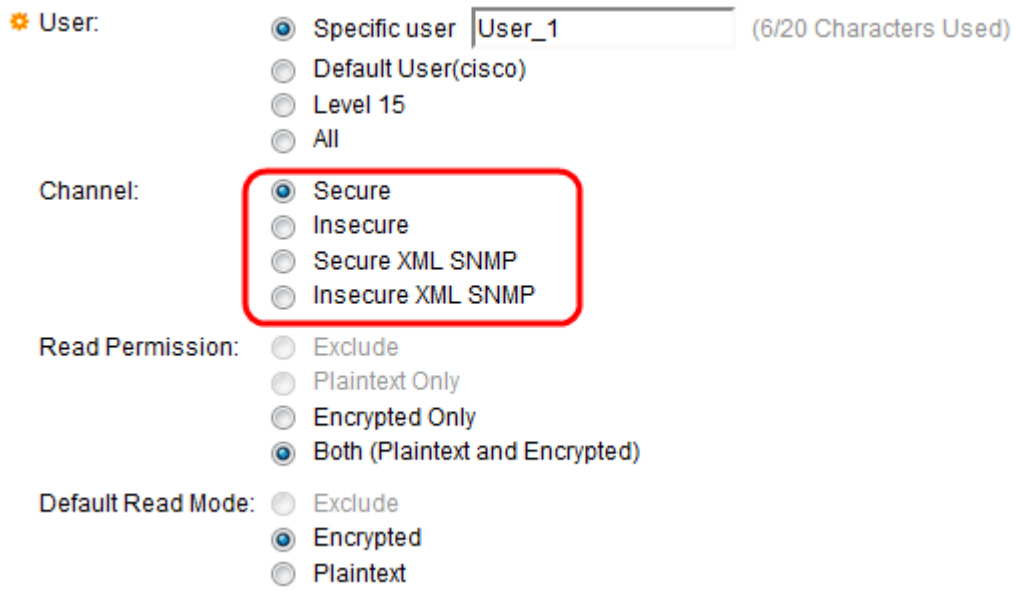


Étape 2. Cliquez sur Add pour ajouter une nouvelle règle disque transistorisé. La fenêtre de *règle disque transistorisé d'ajouter* apparaît.



Étape 3. Cliquez sur la case d'option désirée d'utilisateur à laquelle la règle disque transistorisé apparaît. Les options disponibles sont :

- Utilisateur spécifique — Écrivez le nom d'utilisateur spécifique auquel cette règle s'applique (cet utilisateur ne doit pas nécessairement être défini).
- Utilisateur par défaut (Cisco) — La règle s'applique à l'utilisateur par défaut.
- Niveau 15 — La règle s'applique à tous les utilisateurs avec le niveau de privilège 15. Ici l'utilisateur peut accéder au GUI et peut configurer le commutateur. Pour changer les configurations de privilège référez-vous à la *configuration de compte d'utilisateur d'*article *sur des commutateurs empilables de gamme Sx500*.
- Entièrement la règle s'applique à tous les utilisateurs.



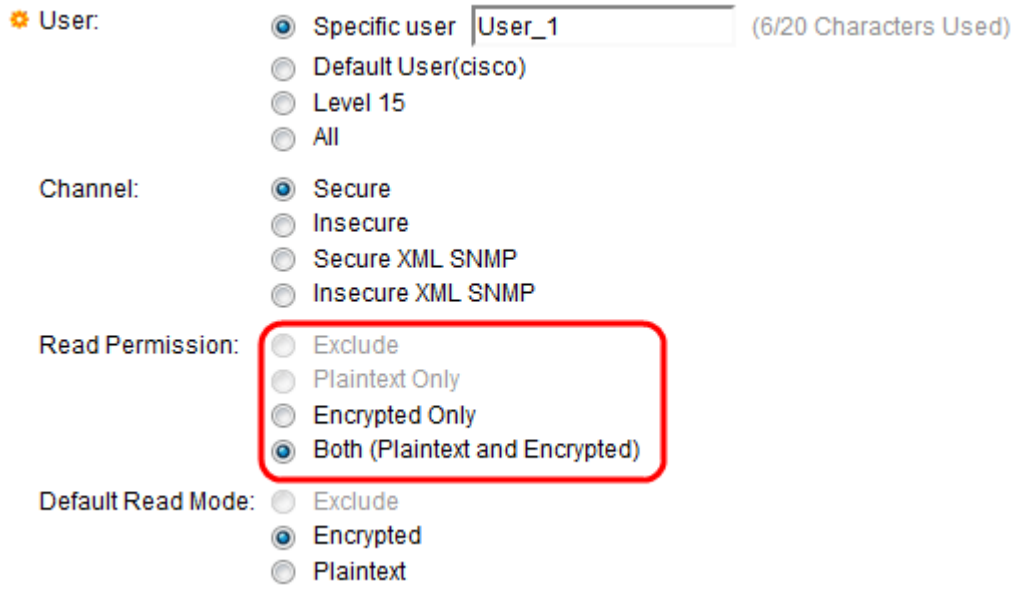
Étape 4. Cliquez sur la case d'option qui correspond au niveau de Sécurité du canal d'entrée auquel la règle applique dans le domaine de la Manche. Les options disponibles sont :

• Sécurisé — Cette règle s'applique seulement aux canaux de sécuriser (console, SCP, SSH, et HTTPS), pas comprenant les canaux SNMP et XML.

• Non sécurisé — Cette règle s'applique seulement aux canaux non sécurisés (telnet, TFTP, et HTTP), pas comprenant les canaux SNMP et XML.

• SNMP XML sécurisé — Cette règle s'applique seulement au XML au-dessus de HTTPS et de SNMPv3 avec l'intimité.

• SNMP XML non sécurisé — Cette règle s'applique seulement au XML au-dessus du HTTP ou le SNMPv1/v2 et le SNMPv3 sans intimité.



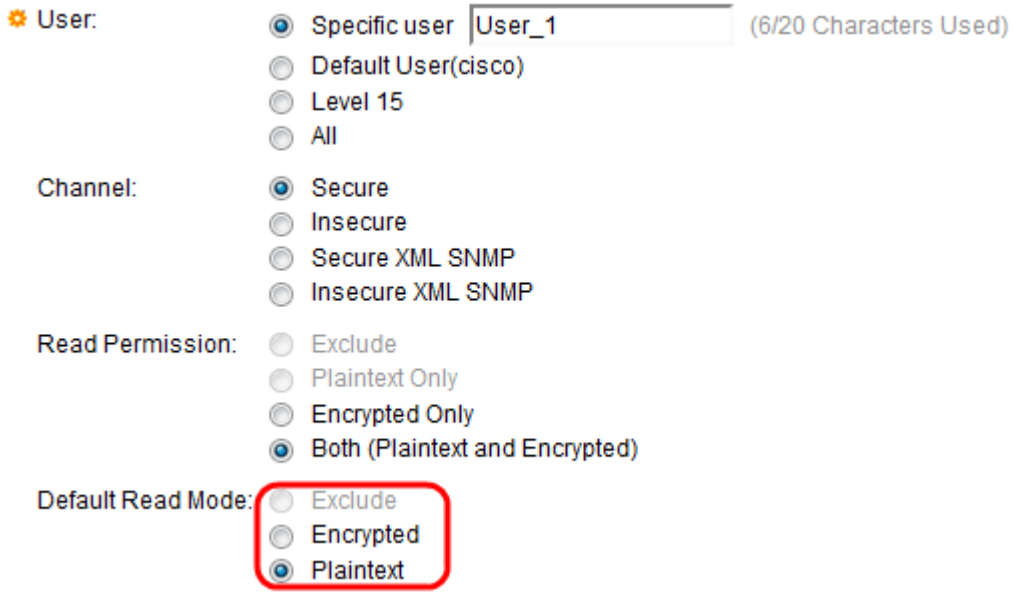
Étape 5. Cliquez sur la case d'option désirée pour définir les autorisations lues associées avec la règle dans le domaine lu d'autorisation. Les options disponibles sont :

• L'excluez — On ne permet pas aux les plus inférieurs de l'autorisation lue et les utilisateurs pour recevoir des données sensibles sous aucune forme. Cette option est disponible seulement si non sécurisé est cliquée sur dans l'étape 4.

• Plaintext seulement — Un niveau supérieur de l'autorisation lue une fois comparé de exclure. Cette option permet aux utilisateurs pour recevoir des données sensibles dans seulement le format de plaintext. Cette option est disponible seulement si non sécurisé est cliquée sur dans l'étape 4.

• Chiffré seulement — Le niveau moyen de l'autorisation lue. Cette option permet aux utilisateurs pour recevoir des données sensibles comme chiffré seulement.

• Chacun des deux (Plaintext et chiffré) — Le de plus haut niveau de l'autorisation lue. Cette option permet aux utilisateurs pour recevoir des autorisations chiffré et de plaintext et est laissée obtenir des données sensibles comme chiffré et sous forme de texte seul.



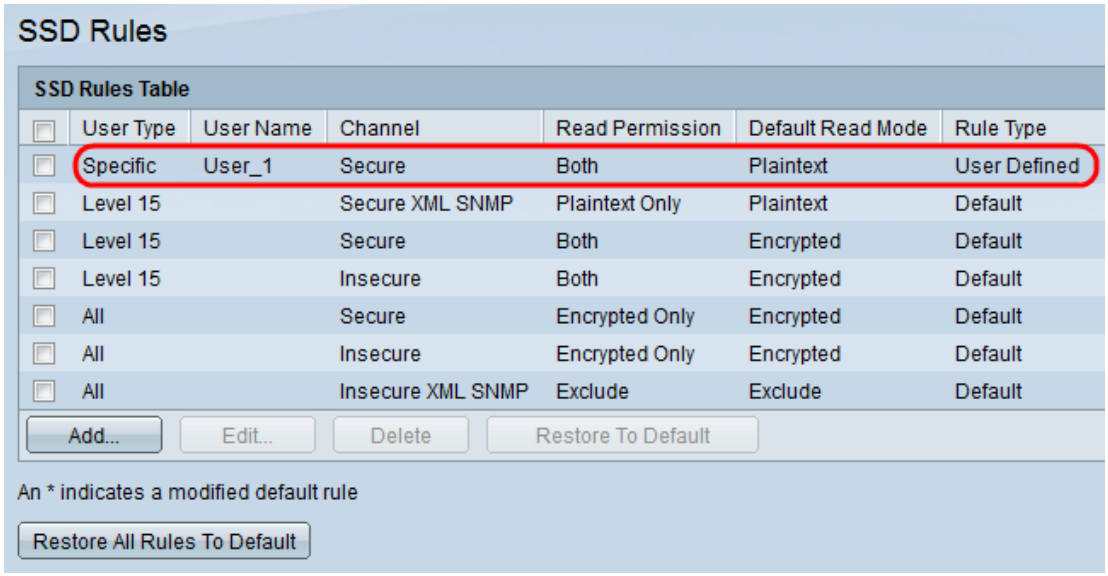
Étape 6. Cliquez sur la case d'option qui correspond au mode indiqué désiré du champ par défaut de mode indiqué. Il définit l'autorisation par défaut donnée à tous les utilisateurs. L'option par défaut de mode lu n'a pas une haute priorité que le champ lu d'autorisation. Les options disponibles sont :

• L'excluez — Ne te permet pas pour lire les données sensibles. Cette option est disponible seulement si non sécurisé est cliquée sur dans l'étape 4.

• Chiffré — Des données sensibles sont présentées chiffrées.

• Plaintext — Des données sensibles sont présentées comme plaintext.

Étape 7. **Sauvegarde de** clic dans la fenêtre de *règle disque transistorisé d'ajouter*. Les modifications sont affichées dans le Tableau de règles disque transistorisé comme affiché ci-dessous :


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