Configuración de reglas de datos confidenciales seguros (SSD) en switches apilables de la serie Sx500

Objetivo

La gestión de datos confidenciales seguros (SSD) se utiliza para administrar datos confidenciales, como contraseñas y claves de forma segura en el switch, rellenar estos datos en otros dispositivos y proteger la configuración automática. El acceso para ver los datos confidenciales como texto simple o cifrado se proporciona en función del nivel de acceso configurado por el usuario y del método de acceso del usuario. En este artículo se explica cómo administrar las reglas SSD en los switches apilables de la serie Sx500.

Nota: Es posible que también desee saber cómo administrar las propiedades de SSD. Para obtener más información, consulte el artículo *Propiedades de datos confidenciales seguros (SSD) en switches apilables de la serie Sx500*.

Dispositivos aplicables

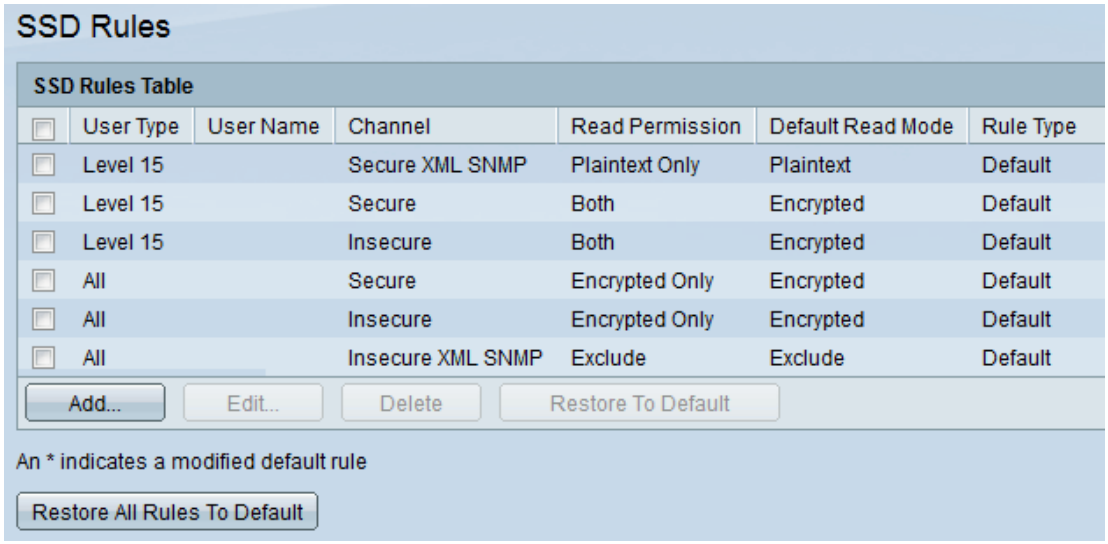
Switches apilables · Sx500 Series

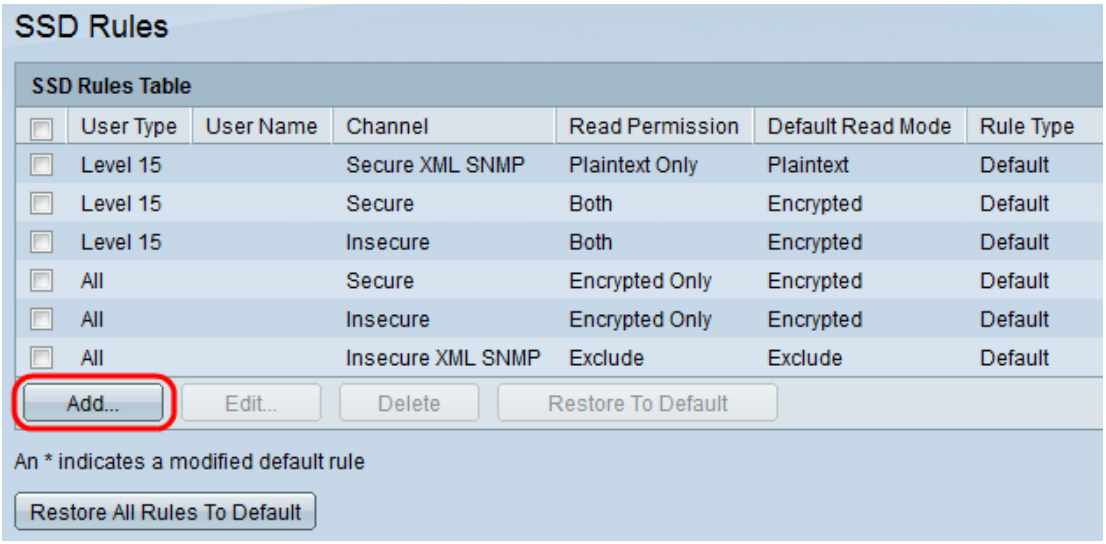
Versión del software

•v1.2.7.76

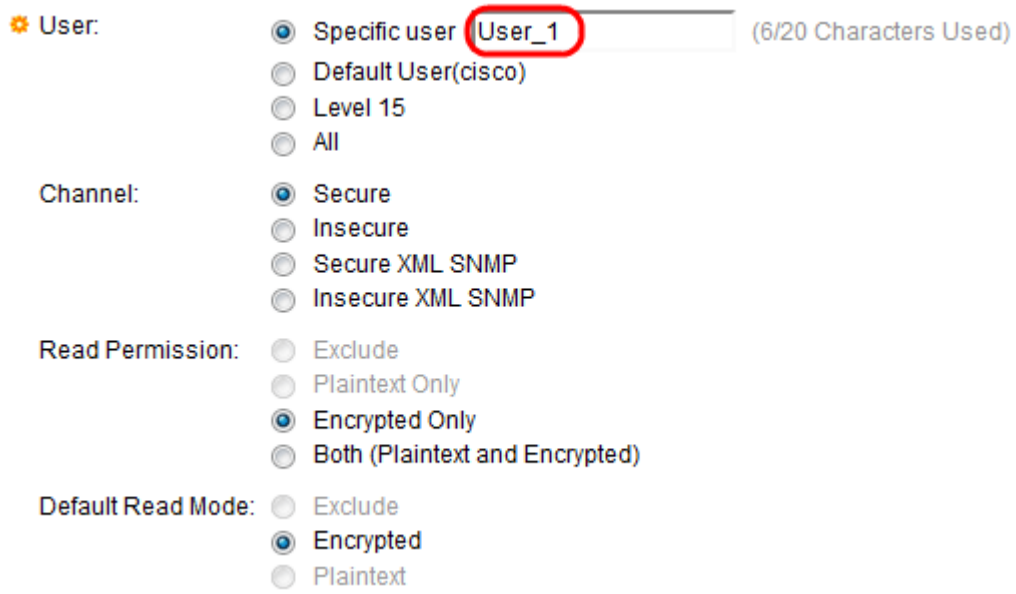
Configuración de reglas SSD

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Security > Secure Sensitive Data Management > SSD Rules**. Se abre la página *Reglas SSD*:





Paso 2. Haga clic en **Agregar** para agregar una nueva regla SSD. Aparece la ventana *Agregar regla SSD*.



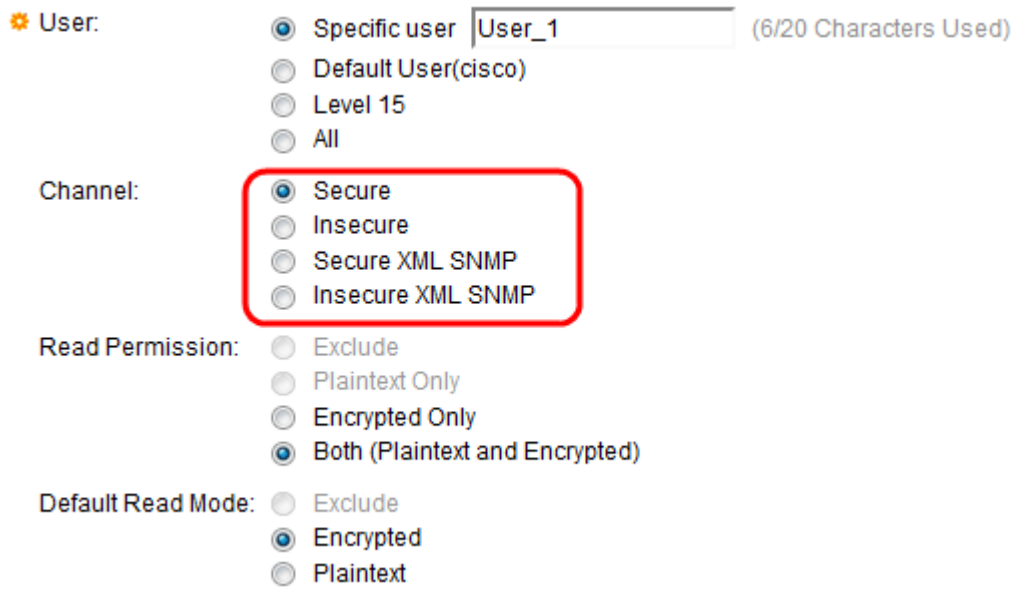
Paso 3. Haga clic en el botón de opción Usuario deseado al que aparece la regla SSD. Las opciones disponibles son:

·usuario específico: introduzca el nombre de usuario específico al que se aplica esta regla (este usuario no tiene que definirse necesariamente).

Usuario predeterminado · (cisco): la regla se aplica al usuario predeterminado.

·Nivel 15: la regla se aplica a todos los usuarios con nivel de privilegio 15. Aquí el usuario puede acceder a la GUI y configurar el switch. Para cambiar la configuración de privilegios, consulte el artículo *Configuración de cuentas de usuario en switches apilables de la serie Sx500*.

·Todos: la regla se aplica a todos los usuarios.



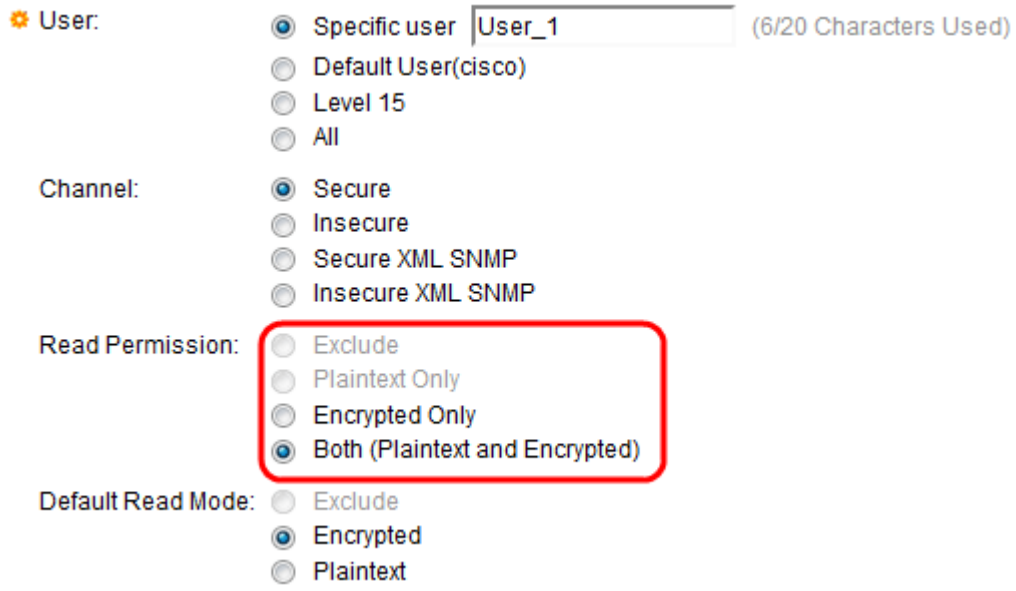
Paso 4. Haga clic en el botón de opción correspondiente al nivel de seguridad del canal de entrada al que se aplica la regla en el campo Canal. Las opciones disponibles son:

·Secure: esta regla se aplica solamente a los canales seguros (consola, SCP, SSH y HTTPS), sin incluir los canales SNMP y XML.

·Insecure: esta regla se aplica solamente a canales inseguros (Telnet, TFTP y HTTP), sin incluir los canales SNMP y XML.

·Secure XML SNMP: esta regla sólo se aplica a XML sobre HTTPS y SNMPv3 con privacidad.

·SNMP XML inseguro: esta regla se aplica sólo a XML sobre HTTP o SNMPv1/v2 y SNMPv3 sin privacidad.



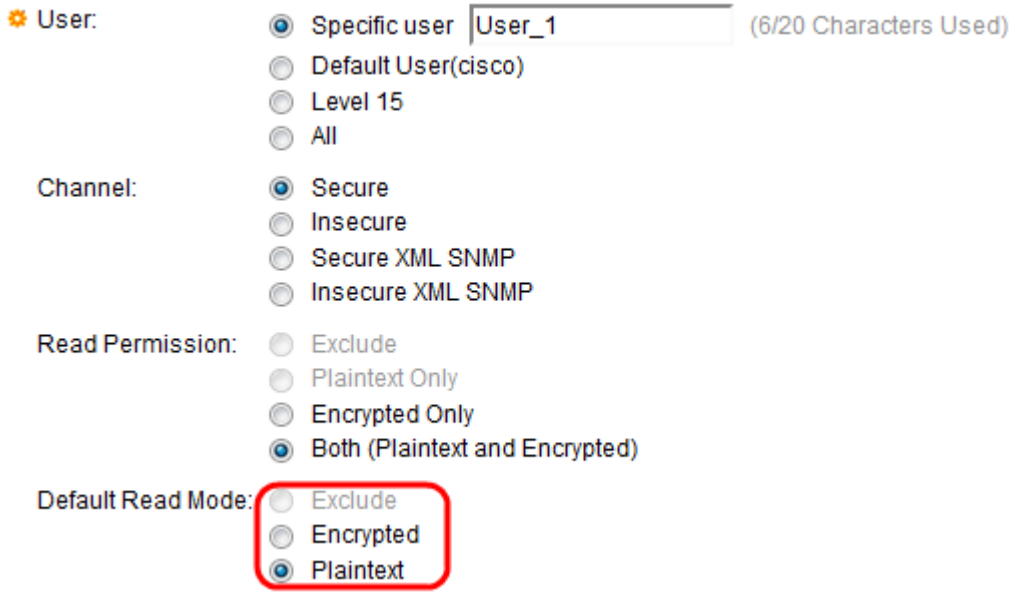
Paso 5. Haga clic en el botón de opción deseado para definir los permisos de lectura asociados a la regla en el campo Permisos de lectura. Las opciones disponibles son:

·Excluir: el nivel más bajo de permiso de lectura y a los usuarios no se les permite recibir datos confidenciales de ninguna forma. Esta opción sólo está disponible si se hace clic en Insecure en el Paso 4.

Sólo texto plano ·: un nivel más alto de permiso de lectura en comparación con Excluir. Esta opción permite a los usuarios recibir datos confidenciales en formato de sólo texto sin formato. Esta opción sólo está disponible si se hace clic en Insecure en el Paso 4.

·Solo cifrado: nivel medio del permiso de lectura. Esta opción permite a los usuarios recibir datos confidenciales sólo como cifrados.

·Ambos (texto sin formato y cifrado): el nivel más alto de permiso de lectura. Esta opción permite a los usuarios recibir permisos cifrados y de texto sin formato y obtener datos confidenciales como formularios cifrados y de texto sin formato.



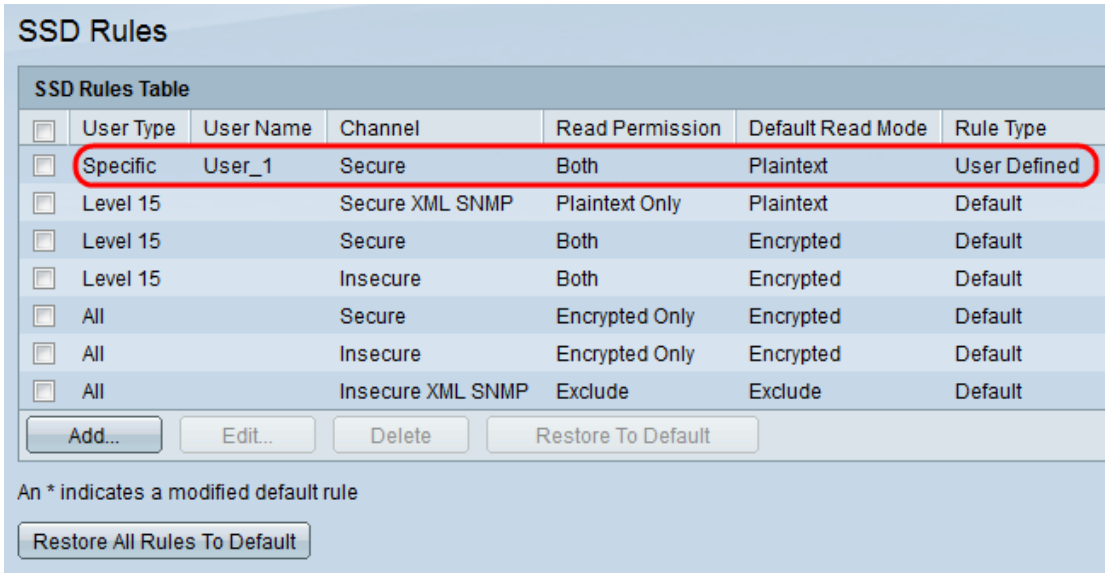
Paso 6. Haga clic en el botón de opción correspondiente al modo de lectura deseado en el campo Modo de lectura predeterminado. Define el permiso predeterminado concedido a todos los usuarios. La opción Modo de lectura predeterminado no tiene una prioridad más alta que el campo Permiso de lectura. Las opciones disponibles son:

·Excluir: no permite leer los datos confidenciales. Esta opción sólo está disponible si se hace clic en Insecure en el Paso 4.

·cifrado: los datos confidenciales se presentan cifrados.

·texto sin formato: los datos confidenciales se presentan como texto sin formato.

Paso 7. Haga clic en **Guardar** en la *ventana Add SSD Rule*. Los cambios se muestran en la Tabla de Reglas de SSD como se muestra a continuación:


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