Creación y gestión de reglas de datos confidenciales seguros (SSD) en switches gestionados serie 200/300

Objetivo

En este artículo se muestra cómo configurar y administrar reglas para Secure Sensitive Data (SSD) en los switches de la serie 200/300.

Dispositivos aplicables

·Switches gestionados serie SF/SG 200 y SF/SG 300

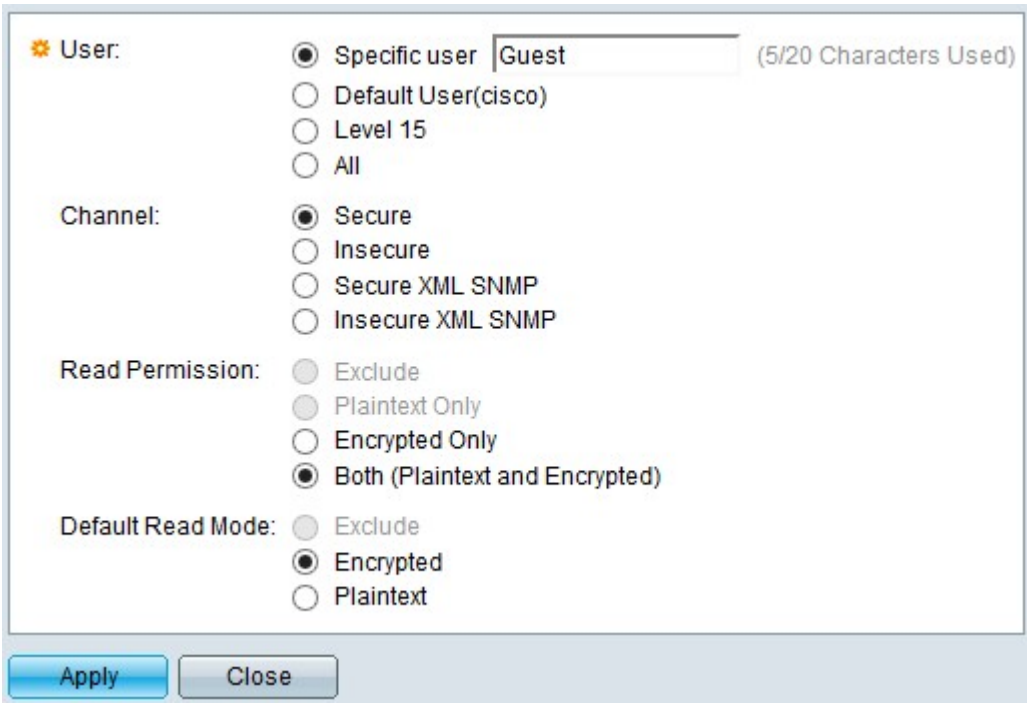
Versión del software

•v1.2.7.76

Reglas de SSD

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

Paso 2. Para crear una nueva regla, haga clic en **Agregar**. Se abre la página *Definición de regla*.



Paso 3. En el campo *Usuario*, seleccione un botón de opción para elegir a qué usuario o usuarios aplicar la regla.

·Usuario específico: introduzca el nombre de usuario específico en el campo si la regla se aplica a un único usuario.

·Usuario predeterminado:. Esta regla se aplica al usuario predeterminado, que está establecido en cisco.

·Nivel 15: esta regla se aplica a todos los usuarios con privilegios de nivel 15.

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

Paso 4. En el campo *Channel*, elija un botón de opción para determinar a qué canal o canales aplicar la regla.

·Segura: hace que esta regla solo se aplique a canales seguros. Esto incluye la consola, SSH y HTTPS, pero no los canales XML.

·Inseguro: hace que esta regla solo se aplique a canales inseguros. Esto incluye Telnet, TFTP y HTTP, pero no los canales XML.

·SNMP de XML seguro: hace que esta regla solo se aplique a XML sobre HTTPS con privacidad.

·SNMP de XML inseguro: hace que esta regla sólo se aplique a XML sobre HTTP o sin privacidad.

Paso 5. En el campo *Permiso de lectura*, seleccione un botón de opción en función de las selecciones anteriores.

·Si en el paso 3 ha elegido Nivel 15 o Todo, haga clic en **Excluir** o **Sólo texto sin formato.**

·Si, en el paso 4, elige SNMP XML seguro o SNMP XML inseguro, haga clic en **Excluir** o **Sólo texto sin formato.**

·Si, en el paso 4, elige Seguro o Inseguro, haga clic en **Sólo cifrado** o **Ambos (texto sin formato y cifrado).**

Paso 6. En el campo *Default Read Mode*, haga clic en **Exclude**, **Encrypted** o **Plaintext.**

Paso 7. Para activar la regla, haga clic en **Apply**. Para cancelar la creación de la regla, haga clic en **Cerrar.**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).