Criação e gerenciamento de regras de dados confidenciais seguros (SSD) em switches gerenciados 200/300 Series

Objetivo

Este artigo mostra como configurar e gerenciar regras para Secure Sensitive Data (SSD) nos switches da série 200/300.

Dispositivos aplicáveis

·Switches gerenciados SF/SG 200 e SF/SG 300 Series

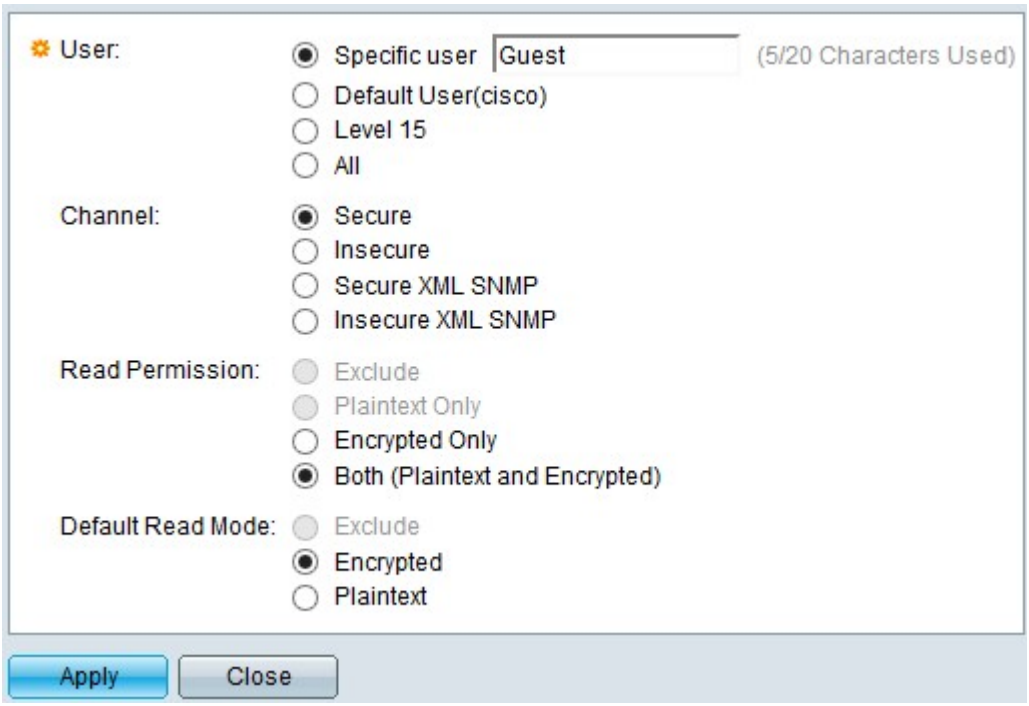
Versão de software

•v1.2.7.76

Regras de SSD

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Security > Secure Sensitive Data Management > SSD Rules**. A página *Regras de SSD* é exibida.

Etapa 2. Para criar uma nova regra, clique em **Adicionar**. A página *Definição de regra* é aberta.



Etapa 3. No campo *Usuário*, selecione um botão de opção para escolher a qual usuário aplicar a regra.

·Usuário específico — Insira o nome de usuário específico no campo se a regra se aplicar a um único usuário.

·Usuário padrão —. Esta regra se aplica ao usuário padrão, que é definido como cisco.

·Nível 15 — Esta regra se aplica a todos os usuários com privilégios de nível 15.

·Todos — Esta regra se aplica a todos os usuários.

Etapa 4. No campo *Channel*, escolha um botão de opção para determinar a que canal(is) aplicar a regra.

·Seguro — Faz com que essa regra se aplique somente a canais seguros. Isso inclui console, SSH e HTTPS, mas não canais XML.

·Inseguro — Faz com que essa regra se aplique somente a canais inseguros. Isso inclui Telnet, TFTP e HTTP, mas não canais XML.

·Secure XML SNMP — Faz com que esta regra se aplique somente a XML sobre HTTPS com privacidade.

·SNMP XML Não Seguro — Faz com que esta regra se aplique somente a XML sobre HTTP ou sem privacidade.

Etapa 5. No campo *Permissão de Leitura*, selecione um botão de opção dependendo de suas seleções anteriores.

·Se, na Etapa 3, você escolher Nível 15 ou Todos, clique em **Excluir** ou **Somente texto simples.**

·Se, na Etapa 4, você escolher Secure XML SNMP ou Insecure XML SNMP, clique em **Exclude** ou **Plaintext Only.**

·Se, na Etapa 4, você escolher Seguro ou Inseguro, clique em **Somente criptografado** ou **Ambos (Texto simples e Criptografado).**

Etapa 6. No campo *Modo de leitura padrão*, clique em **Excluir**, **Criptografado** ou **Texto simples.**

Passo 7. Para ativar a regra, clique em **Aplicar**. Para cancelar a criação da regra, clique em **Fechar.**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.