

Creatie en beheer van Secure Sensitive Data (SSD) - regels op 200/300 Series beheerde Switches

Doel

Dit artikel toont u hoe u regels voor Secure Sensitive Data (SSD) op de switches van de 200/300-serie instelt en beheert.

Toepasselijke apparaten

·SF/SG 200 en SF/SG 300 Series beheerde Switches

Softwareversie

·v1.2.7.76

SSD-regels

Stap 1. Log in op het web configuratie hulpprogramma en kies **Security > Secure Sensitive Data Management > SSD-regels**. De pagina *SSD Rules* verschijnt.

<input type="checkbox"/>	User Type	User Name	Channel	Read Permission	Default Read Mode	Rule Type
<input type="checkbox"/>	Level 15		Secure XML SNMP	Plaintext Only	Plaintext	Default
<input type="checkbox"/>	Level 15		Secure	Both	Encrypted	Default
<input type="checkbox"/>	Level 15		Insecure	Both	Encrypted	Default
<input type="checkbox"/>	All		Secure	Encrypted Only	Encrypted	Default
<input type="checkbox"/>	All		Insecure	Encrypted Only	Encrypted	Default
<input type="checkbox"/>	All		Insecure XML SNMP	Exclude	Exclude	Default

An * indicates a modified default rule

Stap 2. Klik op **Toevoegen** om een nieuwe regel te maken. De pagina *Regeldefinitie* wordt geopend.

User: Specific user (5/20 Characters Used)
 Default User(cisco)
 Level 15
 All
 Channel:
 Secure
 Insecure
 Secure XML SNMP
 Insecure XML SNMP
 Read Permission:
 Exclude
 Plaintext Only
 Encrypted Only
 Both (Plaintext and Encrypted)
 Default Read Mode:
 Exclude
 Encrypted
 Plaintext

Apply Close

Stap 3. Selecteer in het veld *Gebruiker* een keuzerondje om te kiezen op welke gebruiker(s) u de regel wilt toepassen.

- Specifieke gebruiker — Voer de specifieke gebruikersnaam in het veld in als de regel van toepassing is op één gebruiker.
- Standaard gebruiker — Deze regel is van toepassing op de standaardgebruiker, die is ingesteld op cisco.
- Niveau 15 — Deze regel is van toepassing op alle gebruikers met niveau 15 voorrechten.
- Alle — Deze regel is van toepassing op alle gebruikers.

Stap 4. Selecteer in het veld *Kanaal* een keuzerondje om te bepalen op welk(e) kanaal(en) u de regel wilt toepassen.

- Veilig — Maakt deze regel alleen van toepassing op veilige kanalen. Dit omvat console, SSH en HTTPS, maar niet XML-kanalen.
- Onveilig — Maakt deze regel alleen van toepassing op onveilige kanalen. Dit omvat Telnet, TFTP en HTTP, maar niet XML-kanalen.
- Secure XML SNMP — Maakt deze regel alleen van toepassing op XML via HTTPS met privacy.
- Insecure XML SNMP — Maakt deze regel alleen van toepassing op XML via HTTP of zonder privacy.

Stap 5. Selecteer in het veld *Leestoestemming* een keuzerondje afhankelijk van uw vorige selecties.

- Als u in Stap 3 voor Niveau 15 of Alle hebt gekozen, klikt u op **Alleen uitsluiten** of **Alleen onbewerkte tekst**.
- Als u in Stap 4 voor Secure XML SNMP of Insecure XML SNMP hebt gekozen, klikt u op **Uitsluiten** of **Alleen onbewerkte tekst**.

·Als u in Stap 4 voor Secure of Insecure hebt gekozen, klikt u op **Alleen versleuteld** of op **Beide** (zowel Plaintext als Encrypted).

Stap 6. Klik in het veld *Standaard leesmodus* op **Uitsluiten**, **Versleuteld** of **Plaintext**.

Stap 7. Klik op **Toepassen** om de regel te activeren. Klik op **Sluiten** om het maken van de regel te annuleren.

SSD Rules

SSD Rules Table						
<input type="checkbox"/>	User Type	User Name	Channel	Read Permission	Default Read Mode	Rule Type
<input checked="" type="checkbox"/>	Specific	Guest	Secure	Both	Encrypted	User Defined
<input type="checkbox"/>	Level 15		Secure XML SNMP	Plaintext Only	Plaintext	Default
<input type="checkbox"/>	Level 15		Secure	Both	Encrypted	Default
<input type="checkbox"/>	Level 15		Insecure	Both	Encrypted	Default
<input type="checkbox"/>	All		Secure	Encrypted Only	Encrypted	Default
<input type="checkbox"/>	All		Insecure	Encrypted Only	Encrypted	Default
<input type="checkbox"/>	All		Insecure XML SNMP	Exclude	Exclude	Default

An * indicates a modified default rule

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.