

Secure Sensitive Data (SSD)-regels configuratie voor SX500 Series Stackable Switches

Doel

Secure Sensitive Data (SSD) Management wordt gebruikt om gevoelige gegevens zoals wachtwoorden en toetsen veilig op de switch te beheren, deze gegevens aan andere apparaten te laten bevolken en de automatische configuratie te beveiligen. Toegang om de gevoelige gegevens als tekst of versleuteld te bekijken wordt verleend op basis van het door de gebruiker ingestelde toegangsniveau en de toegangsmethode van de gebruiker. Dit artikel legt uit hoe de SSD-regels voor de SX500 Series Stackable Switches moeten worden beheerd.

Opmerking: Het kan ook zijn dat u wilt weten hoe u de SSD-eigenschappen beheert. Raadpleeg voor meer informatie het artikel *Secure Sensitive Data (SSD) Properties op SX500 Series Stackable Switches*.

Toepasselijke apparaten

- SX500 Series Stackable-switches

Softwareversie

- v1.2.7.76

Configuratie van SSD-regels

Stap 1. Meld u aan bij het web configuratieprogramma en kies **Security > Secure Sensitive Data Management > SSD-regels**. De pagina *SSD-regels* wordt geopend:

<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

SSD Rules

SSD Rules Table						
<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 **Add** om een nieuwe SSD-regel toe te voegen. Het venster *Add SSD Rule* verschijnt.

User:
 Specific user (6/20 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

Stap 3. Klik op het gewenste keuzerondje waarop de SSD-regel wordt weergegeven. De beschikbare opties zijn:

- Specifieke gebruiker — Voer de specifieke gebruikersnaam in waarop deze regel van toepassing is (deze gebruiker hoeft niet noodzakelijkerwijs te worden gedefinieerd).
- Standaard gebruiker (cisco) - de regel is van toepassing op de standaardgebruiker.
- Niveau 15 — De regel is van toepassing op alle gebruikers met voorkeursniveau 15. Hier kan de gebruiker de GUI benaderen en de schakelaar configureren. Om de instellingen van het voorrecht te veranderen raadpleegt u de *gebruikersaccountconfiguratie van artikel SX500 Series Stackable-switches*.
- Alle — De regel is van toepassing op alle gebruikers.

User: Specific user (6/20 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

Stap 4. Klik op de radioknop die overeenkomt met het beveiligingsniveau van het invoerkanaal waarop de regel van toepassing is in het veld Kanaal. De beschikbare opties zijn:

- Beveiligd — Deze regel is alleen van toepassing op beveiligde kanalen (console, SCP, SSH en HTTPS), met uitzondering van SNMP en XML kanalen.
- Onveilig — Deze regel is alleen van toepassing op onveilige kanalen (telnet, TFTP en HTTP), zonder de SNMP en XML kanalen.
- Secure XML SNMP — Deze regel is alleen van toepassing op XML over HTTPS en SNMPv3 met privacy.
- Onveilig XML SNMP — Deze regel is alleen van toepassing op XML via HTTP of SNMPv1/v2 en SNMPv3 zonder privacy.

User: Specific user (6/20 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

Stap 5. Klik op het gewenste keuzerondje om de leesrechten te definiëren die aan de regel zijn gekoppeld in het veld Lezen. De beschikbare opties zijn:

- Uitsluiten — Het laagste niveau van leesrechten en de gebruikers mogen geen gevoelige gegevens ontvangen. Deze optie is alleen beschikbaar indien op onveilig is gedrukt in Stap

4.

- Alleen tekst — Een hoger leesniveau in vergelijking met uitsluiten. Met deze optie kunnen gebruikers gevoelige gegevens alleen in tekstindeling ontvangen. Deze optie is alleen beschikbaar indien op onveilig is gedrukt in Stap 4.
- Alleen versleuteld — middenniveau van de leestoestemming. Met deze optie kunnen gebruikers alleen gevoelige gegevens ontvangen als versleuteld.
- Beide (Plaintext en Encrypted) — het hoogste niveau van leestoestemming. Met deze optie kunnen de gebruikers zowel gecodeerde als intekstrechten ontvangen en is het toegestaan om gevoelige gegevens als gecodeerd en intekstformulier te verkrijgen.

 User: Specific user (6/20 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

Stap 6. Klik op de radioknop die overeenkomt met de gewenste leesmodus in het veld Default Read Mode. Het definieert de standaardtoestemming die aan alle gebruikers wordt gegeven. De optie Standaardleesmodus heeft geen hogere prioriteit dan het veld Lezen Toestemming. De beschikbare opties zijn:

- Sluit - staat u niet toe om de gevoelige gegevens te lezen. Deze optie is alleen beschikbaar indien op onveilig is gedrukt in Stap 4.
- Versleuteld — Gevoelige gegevens worden versleuteld.
- Plaintext — Gevoelige gegevens worden gepresenteerd als kladtekst.

Stap 7. Klik op **Opslaan** in het venster *Toevoegen van de SDD-regel*. De wijzigingen worden in de tabel SSD-regels weergegeven zoals hieronder wordt weergegeven:

SSD Rules

SSD Rules Table

<input type="checkbox"/>	User Type	User Name	Channel	Read Permission	Default Read Mode	Rule Type
<input type="checkbox"/>	Specific	User_1	Secure	Both	Plaintext	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

Add...

Edit...

Delete

Restore To Default

An * indicates a modified default rule

Restore All Rules To Default