# Propriedades de Dados Sensíveis de Segurança (SSD - Secure Sensitive Data) em Switches Empilháveis Sx500 Series

## Objetivo

O Gerenciamento de Dados Sensíveis de Segurança (SSD - Secure Sensitive Data) é usado para gerenciar dados confidenciais como senhas e chaves com segurança no switch. Essas informações devem ser protegidas quando são enviadas de um dispositivo para outro. O nível de acesso do usuário determina como os dados confidenciais podem ser visualizados, seja como texto simples ou dados criptografados. As propriedades SSD são um conjunto de parâmetros em conjunto com as regras SSD que controlam as configurações, como o modo como os dados confidenciais são criptografados, a força da segurança nos arquivos de configuração e como os dados confidenciais são visualizados na sessão atual.

O objetivo deste documento é ajudar a configurar as propriedades de dados confidenciais seguros (SSD) em switches empilháveis Sx500 Series.

#### Dispositivos aplicáveis

Switches Empilháveis Sx500 Series

#### Versão de software

•1.3.0.62

### **Propriedades SSD**

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Security > Secure Sensitive Data Management > Properties.** A página *Propriedades* é aberta:

Persistent Settings		
Current Local Passphrase Type:	Default	
Configuration File Passphrase Control:	•	Unrestricted Restricted
Configuration File Integrity Control:		Enable
Current Session Settings		
Read Mode:	0	Plaintext
	۲	Encrypted

Note: O campo Tipo de senha local atual exibe o tipo de senha local inicialmente definida.

Etapa 2. No campo Configuration File Passphrase Control (Controle de senha de arquivo de configuração), clique no botão de opção do tipo desejado de controle de senha. O controle de senha de arquivo oferece proteção extra à senha definida pelo usuário e aos dados criptografados com a senha definida pelo usuário.

Unrestricted — A senha definida pelo usuário está incluída no arquivo de configuração que é enviado de um dispositivo para outro.

Restrito — A senha definida pelo usuário não está incluída no arquivo de configuração.

Etapa 3. (Opcional) Para habilitar o controle de integridade do arquivo, marque a caixa de seleção **Habilitar** no campo Controle de integridade do arquivo de configuração. Esta opção protege o arquivo de configuração da modificação.

Etapa 4. No campo Modo de leitura, clique no botão de opção desejado. As opções disponíveis são:

Texto sem formatação — Os dados confidenciais são exibidos como texto sem formatação.

Criptografado — Os dados são exibidos na forma criptografada.

Etapa 5. Clique em Apply.

#### Alterar senha local

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Security > Secure Sensitive Data Management > Properties.** A página *Propriedades* é aberta:

Properties	
Persistent Settings	
Current Local Passphrase Type:	Default
Configuration File Passphrase Control:	<ul> <li>Unrestricted</li> <li>Restricted</li> </ul>
Configuration File Integrity Control:	Enable
Current Session Settings	
Read Mode:	O Plaintext
	Encrypted
Apply Cancel Change	e Local Passphrase

Etapa 2. Clique em **Alterar senha local** para alterar a senha local atual. A página *Alterar senha local* é aberta:

Change Local Passphra	se					
The minimum requirements for Local Passphrase are as follows: • Should be at least 8 characters up to 16 characters. • Should be at least one upper case character, one lower case character, one numeric number, and one special charactere e.g. #,\$.						
Current Local Passphrase Type: Default						
O Local Passphrase:	Default     User Defined (Plaintext)     Confirm Passphrase	(0/16 Characters Used)				
Apply Cancel Back						

Note: O campo Tipo de senha local atual exibe a senha local atual.

Change Local Passphr	ase					
The minimum requirements for Local Passphrase are as follows: • Should be at least 8 characters up to 16 characters. • Should be at least one upper case character, one lower case character, one numeric number, and one special charactere e.g. #,\$.						
Current Local Passphrase Type: Default						
Cocal Passphrase:	O Default					
	<ul> <li>User Defined (Plaintext)</li> </ul>	•••••	(10/16 Characters Used)			
	Confirm Passphrase	•••••				
Apply Cancel	Back					

Etapa 3. No campo Senha local, clique no botão de opção da senha local desejada:

Default (Padrão) — Atribui a senha padrão.

Definido pelo usuário (Texto simples) — Insira a senha desejada. Deve ter entre 8 e 16 caracteres e incluir caracteres em maiúsculas e em minúsculas, um número e um caractere especial.

- Confirmar senha — Insira novamente a senha definida pelo usuário.

Etapa 4. Clique em Apply.