

Sx500 Series Stackable Switch의 SSD(Secure Sensitive Data) 속성

목표

SSD(Secure Sensitive Data) 관리는 비밀번호와 키 같은 민감한 데이터를 스위치에서 안전하게 관리하는 데 사용됩니다. 이 정보는 한 디바이스에서 다른 디바이스로 전송될 때 보호되어야 합니다. 사용자의 액세스 레벨은 민감한 데이터를 일반 텍스트 또는 암호화된 데이터로 보는 방법을 결정합니다. SSD 속성은 SSD 규칙과 함께 매개 변수 집합으로, 민감한 데이터의 암호화 방식, 구성 파일의 보안 수준, 현재 세션 내에서 민감한 데이터를 보는 방법 등의 설정을 제어합니다.

이 문서의 목적은 Sx500 Series Stackable Switch에서 SSD(Secure Sensitive Data) 속성을 구성하는 것입니다.

적용 가능한 디바이스

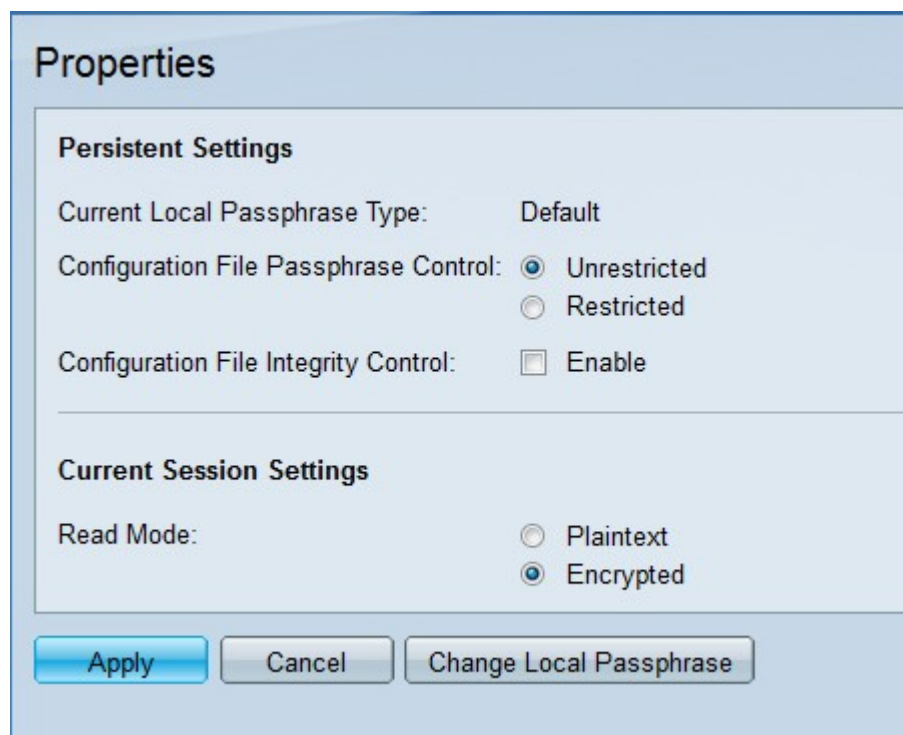
·Sx500 Series Stackable Switch

소프트웨어 버전

·1.3.0.62

SSD 속성

1단계. 웹 구성 유틸리티에 로그인하고 보안 > 보안 중요 데이터 관리 > 속성을 선택합니다. 등록 정보 페이지가 열립니다.



The screenshot shows a 'Properties' dialog box with two main sections: 'Persistent Settings' and 'Current Session Settings'. In 'Persistent Settings', 'Current Local Passphrase Type' is set to 'Default', 'Configuration File Passphrase Control' has 'Unrestricted' selected (indicated by a blue dot), and 'Configuration File Integrity Control' has 'Enable' selected (indicated by a checked checkbox). In 'Current Session Settings', 'Read Mode' has 'Encrypted' selected (indicated by a blue dot). At the bottom, there are three buttons: 'Apply' (highlighted in blue), 'Cancel', and 'Change Local Passphrase'.

참고:Current Local Passphrase Type(현재 로컬 패스프레이즈 유형) 필드는 처음에 설정된 로

컬 패스프레이즈의 유형을 표시합니다.

2단계. Configuration File Passphrase Control(컨피그레이션 파일 패스프레이즈 제어) 필드에서 원하는 유형의 패스프레이즈 제어 라디오 버튼을 클릭합니다.파일 패스프레이즈 제어는 사용자 정의 패스프레이즈 및 사용자 정의 패스프레이즈로 암호화된 데이터에 대한 추가 보호를 제공합니다.

·제한 없음 — 사용자 정의 패스프레이즈가 한 디바이스에서 다른 디바이스로 전송되는 구성 파일에 포함됩니다.

·제한됨 — 사용자 정의 패스프레이즈가 컨피그레이션 파일에 포함되지 않습니다.

3단계. (선택 사항) 파일 무결성 제어를 활성화하려면 Configuration File Integrity Control(컨피그레이션 파일 무결성 제어) 필드에서 Enable(활성화) 확인란을 선택합니다.이 옵션은 컨피그레이션 파일을 수정하지 못하도록 보호합니다.

4단계. Read Mode(읽기 모드) 필드에서 원하는 라디오 버튼을 클릭합니다.사용 가능한 옵션은 다음과 같습니다.

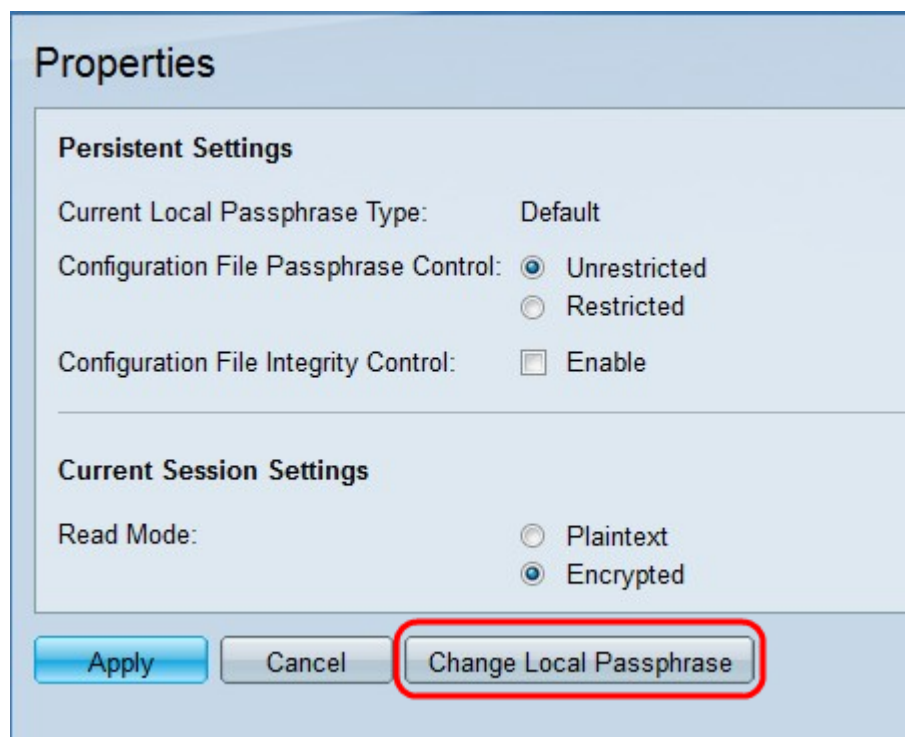
·일반 텍스트 — 민감한 데이터는 일반 텍스트로 표시됩니다.

·암호화됨 — 데이터가 암호화된 형식으로 표시됩니다.

5단계. 적용을 누릅니다.

로컬 암호 변경

1단계. 웹 구성 유틸리티에 로그인하고 보안 > 보안 중요 데이터 관리 > 속성을 선택합니다.등록 정보 페이지가 열립니다.



The image shows a 'Properties' dialog box with two sections: 'Persistent Settings' and 'Current Session Settings'. In 'Persistent Settings', 'Current Local Passphrase Type' is set to 'Default', 'Configuration File Passphrase Control' has 'Unrestricted' selected, and 'Configuration File Integrity Control' has 'Enable' checked. In 'Current Session Settings', 'Read Mode' has 'Encrypted' selected. At the bottom, there are three buttons: 'Apply', 'Cancel', and 'Change Local Passphrase', with the last one highlighted by a red rectangle.

2단계. 현재 로컬 암호를 변경하려면 로컬 암호 변경을 누릅니다. [로컬 암호 변경] 페이지가 열립니다.

Change Local Passphrase

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 character e.g. #,\$.

Current Local Passphrase Type: Default

Local Passphrase: ☒ Default ☐ User Defined (Plaintext) (0/16 Characters Used)

Confirm Passphrase

참고: 현재 로컬 암호 유형 필드는 현재 로컬 암호를 표시합니다.

Change Local Passphrase

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 character e.g. #,\$.

Current Local Passphrase Type: Default

Local Passphrase: ☐ Default ☒ User Defined (Plaintext) (10/16 Characters Used)

Confirm Passphrase

3단계. Local Passphrase(로컬 암호) 필드에서 원하는 로컬 패스프레이즈의 라디오 버튼을 클릭합니다.

· 기본값 — 기본 패스프레이즈가 할당됩니다.

· 사용자 정의(일반 텍스트) — 원하는 암호를 입력합니다. 8자에서 16자 사이여야 하며 대/소문자, 숫자 및 특수 문자를 포함해야 합니다.

- 암호 확인 — 사용자 정의 암호를 다시 입력합니다.

4단계. 적용을 클릭합니다.