Management Access Authentication auf Managed Switches der Serien 200 und 300

Ziel

Verwaltungszugriffsmodi wie SSH, Konsole, Telnet, HTTP und HTTPS ermöglichen es Benutzern, auf ein Gerät zuzugreifen. Zur Verbesserung der Sicherheit kann eine Authentifizierung der Benutzer erforderlich sein. Die Managed Switches der Serien 200 und 300 können lokal oder auf einem TACACS+- oder RADIUS-Server authentifiziert werden. In diesem Dokument wird erläutert, wie Sie den Managed Switches der Serien 200 und 300 eine Authentifizierungsmethode zuweisen.

Unterstützte Geräte

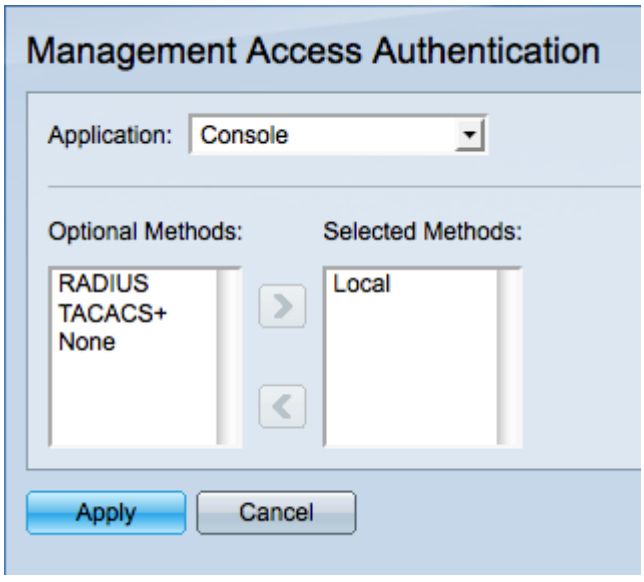
- Managed Switches der Serien SF/SG 200 und SF/SG 300

Software-Version

•1.3.0.62

Authentifizierung des Managementzugriffs

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > Management Access Authentication aus**. Die Seite *Management Access Authentication* wird geöffnet:



Schritt 2: Wählen Sie aus der Dropdown-Liste Anwendung den Anwendungstyp aus, dem Sie die Authentifizierung zuweisen möchten. Mögliche Anwendungen sind:

- Konsole - Ermöglicht die Verwaltung des Switches über eine Konsolenschnittstelle. Ermöglicht Ihnen, eine Verbindung zum Switch herzustellen und einige Konfigurationen durchzuführen, selbst wenn die IP-Adresse des Switches nicht bekannt ist.

- Telnet - Ein zeichenbasiertes Kommunikationsprotokoll, mit dem Sie eine Remote-

Verbindung zum Switch über ein TCP/IP-Netzwerk herstellen können. Telnet wird aufgrund der fehlenden Verschlüsselung nicht empfohlen.

- Secure Telnet (SSH) - Führt die gleichen Funktionen wie Telnet und Verschlüsselung aus. Für Remote-Verbindungen wird SSH empfohlen.

- HTTP — Protokoll, das den Zugriff auf die grafische Benutzeroberfläche (GUI) des Switches ermöglicht. Dies steht im Gegensatz zu Telnet und SSH, die auf Eingabeaufforderungen basieren.

- Sicheres HTTP (HTTPS) — Führt die gleichen Funktionen wie HTTP durch und fügt eine sichere Kommunikation hinzu.

Schritt 3: Wählen Sie eine Authentifizierungsmethode aus der Liste der optionalen Methoden aus, und klicken Sie dann auf die Schaltfläche **>**, um sie in die Liste der ausgewählten Methoden zu verschieben. Unterschiedliche Methoden bieten unterschiedliche Sicherheitsstufen.

Hinweis: Die Reihenfolge, in der die Authentifizierungsmethoden ausgewählt werden, ist die Reihenfolge, in der die Benutzerauthentifizierung erfolgt. Wenn RADIUS vor local ausgewählt wird, versucht das Gerät, den Benutzer vor der lokalen Methode über einen RADIUS-Server zu authentifizieren.

- RADIUS - RADIUS verschlüsselt nur das Passwort. Die Authentifizierung erfolgt auf einem RADIUS-Server und erfordert einen konfigurierten RADIUS-Server.

- TACACS+ - TACACS+ verschlüsselt alle Daten während der Authentifizierung. Die Authentifizierung erfolgt auf einem TACACS+-Server und erfordert einen konfigurierten TACACS+-Server.

- Keine - Für den Zugriff auf den Switch ist keine Authentifizierung erforderlich.

- Lokal - Die Benutzerinformationen werden durch die auf dem Switch gespeicherten Informationen verifiziert.

Schritt 4: Klicken Sie auf **Anwenden**, um die Authentifizierungseinstellungen zu speichern, oder auf **Abbrechen**, um die Änderungen abzubrechen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.