# Auslösen von Kopien der Konfigurationsdatei auf einen TFTP-Server über SNMP

## Ziel

Ziel dieses Artikels ist es, die Schritte zu beschreiben, die das Kopieren von Konfigurationsdateien von einem Cisco Business Switch über das Simple Network Management Protocol (SNMP) auslösen.

## Unterstützte Geräte

- Catalyst 1200-Serie
- Catalyst 1300-Serie
- Serie CBS 250
- Serie CBS 350

### Einleitung

Konfigurationsdateien werden normalerweise über die grafische Benutzeroberfläche (GUI) oder die Befehlszeilenschnittstelle (CLI) von einem Switch kopiert. Eine ungewöhnlichere Methode besteht darin, den Kopiervorgang über SNMP auszulösen.

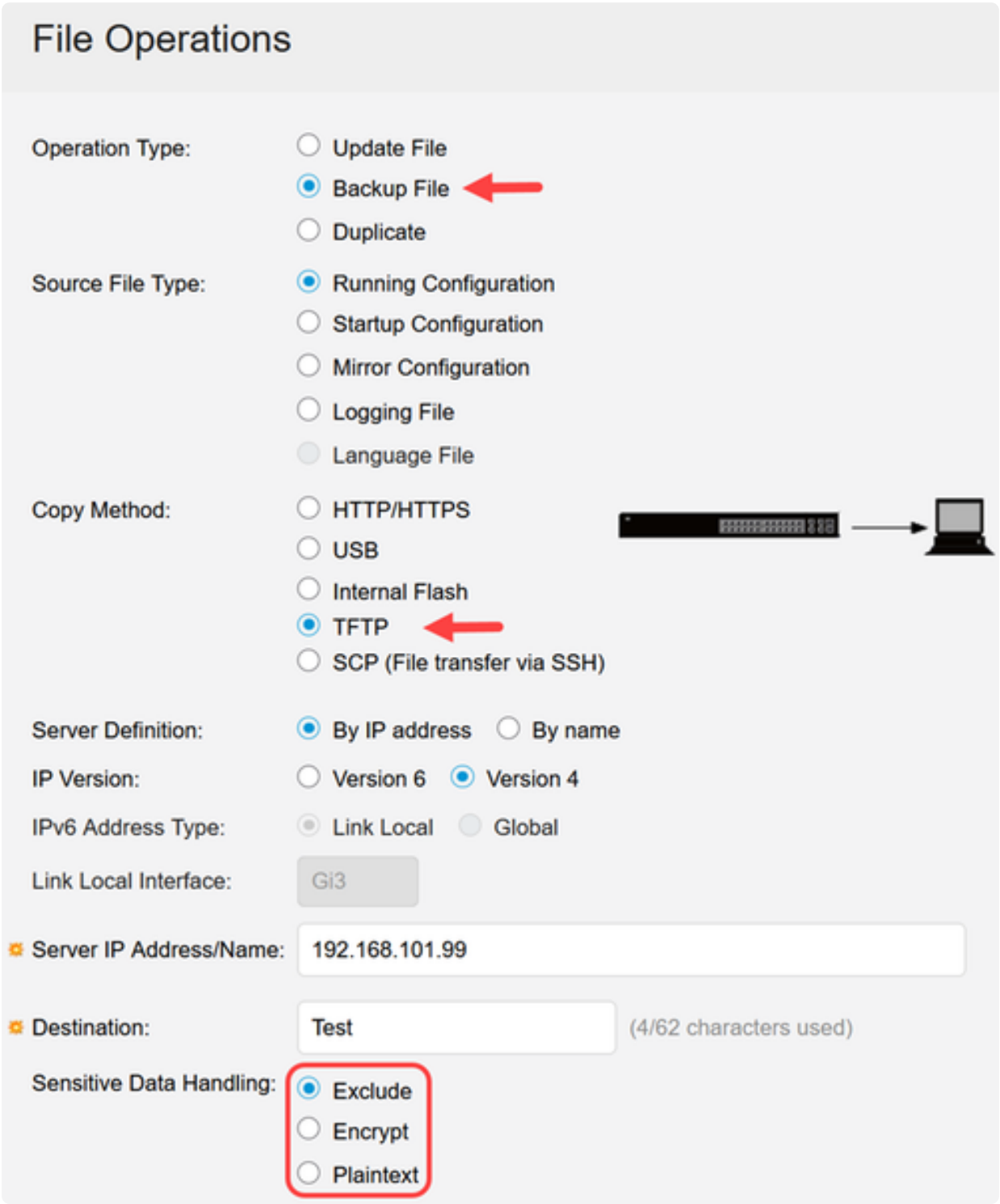
## Verarbeitung vertraulicher Daten

Beim Kopieren einer Konfigurationsdatei, die vertrauliche Daten enthält, kann der Kopiervorgang vertrauliche Daten ausschließen, sie in verschlüsselter Form einschließen, sie als Klartext einschließen oder eine Standardmethode verwenden. Die Angabe des Umgangs mit vertraulichen Daten ist optional. Die Standardeinstellung wird verwendet, wenn sie nicht angegeben wird.

### GUI

Um über die GUI auf das Menü für die Verarbeitung vertraulicher Daten zuzugreifen, navigieren Sie zu Administration > File Operations > File Management menu.

- Ausschließen - um vertrauliche Daten auszuschließen
- Verschlüsseln - um vertrauliche Daten zu verschlüsseln
- Nur-Text - um vertrauliche Daten im Klartext anzuzeigen.




**Note:**

Die Option für vertrauliche Daten wird nur im Modus Backup file für TFTP oder SCP angezeigt.

CLI

In der Befehlszeile kann der Befehl copy verwendet werden:

```
copy {running-config | startup-config} dst-url [exclude | include-
encrypted | include-plaintext]
```

Beispiele:

```
copy running-config tftp://192.168.101.99/destination-file.txt exclude
```

Der Standardwert ist der für den SSD-Sitzungslesemodus (Secure Sensitive Data) festgelegte Wert. Um den aktuellen Modus anzuzeigen, geben Sie show ssd session ein, oder geben show running-config ein, und suchen Sie nach der Datei-SSD-Anzeige. Mit den Werkseinstellungen wird der erwartete SSD-Sitzungslesemodus verschlüsselt.

```
show ssd session
```

```
show running-config | include SSD
```

Wenn der Befehl copy eingegeben wurde, ohne dass eine Option angegeben wurde, würde er kopieren, als ob "include-encrypted" gewählt wurde.

```
copy running-config tftp://192.168.101.99/destination-file.txt
```

Der Sitzungslesewert kann jedoch geändert werden:

```
ssd session read {exclude | encrypted | plaintext}
```

Dieser Befehl beeinflusst die Ausgabe von show running-config und show startup-config und fungiert als Standardwert für die Verarbeitung vertraulicher Daten durch den Befehl copy.

Beispiele:

```
ssd session read plaintext

exit

copy running-config tftp://192.168.101.99/destination-file.txt
```

Die resultierende Datei enthält vertrauliche Daten im Klartext, ebenso wie die Ausgabe von "show running-config" und "show startup-config". Daher sollte der SSD-Sitzungs-Lesemodus mit Vorsicht angewendet werden. Am sichersten ist es, es beim Standard zu belassen.

> **Note:**
> Wenn die Ausgabe von show running-config oder show startup-config nicht alles anzeigt, was erwartet wird, z. B. SNMP v3-Benutzer mit verschlüsselten Anmeldeinformationen, die in der GUI sichtbar sind, stellen Sie sicher, dass der Lesewert für die SSD-Sitzung nicht auf "exclude" gesetzt ist.

## SNMP

Die Switches der Serien Catalyst 1200/Catalyst 1300/CBSx50 verwenden den SNMP-Objektbezeichner (OID) rlCopyOptionsRequestedSsdAccess, um die Option für vertrauliche Daten zu steuern. Das Objekt ist eine ganze Zahl, und auf den ersten Blick sehen die Werte, die es akzeptiert, denen des Befehls copy ähnlich:

- 1: ausschließen
- 2: inkl. verschlüsselt
- 3: include-decrypted (wie "include-plaintext" in der Kommandozeile)
- 4: standard

Option 3, mit der vertrauliche Daten im Klartext kopiert werden, kann mit SNMP v2c nicht verwendet werden. Sie kann auch nicht mit SNMP v3 verwendet werden, es sei denn, sowohl Authentifizierung als auch Datenschutz (authPriv) werden verwendet.

> **Note:**
> Es ist keine gute Idee, die Klartextoption so festzulegen, dass die Datei mit einem unsicheren Protokoll wie TFTP kopiert wird.

SNMP v3 mit authPriv wird nur zum Auslösen der Kopie verwendet. Die Datenschutzeinstellungen sind daher für den Schutz der Konfigurationsdatei selbst während der Übertragung nicht hilfreich. Das Kopieren mit Secure Copy Protocol (SCP) beispielsweise wäre sicherer.

Option 4, die "default"-Option, verhält sich nicht so, wie man erwarten könnte. Er funktioniert nicht wie der Befehl copy, und der SSD-Lese-Sitzungswert hat keinerlei Einfluss auf das Ergebnis copy, wenn SNMP verwendet wird. Stattdessen entspricht Option 4 Option 1 (ausschließen), mit einer Ausnahme: Bei Verwendung von SNMP v3

mit authPriv entspricht Option 4 Option 3 (Klartext).

Das Verhalten ist in der folgenden Tabelle zusammengefasst:

| | 1 (ausschließen) | 2 (verschlüsselt) | 3 (Klartext) | standard |
|---|---|---|---|---|
| CLI-Text | ausgeschlossen | verschlüsselt | Klartext | SSD-Wert |
| SNMP v2c | ausgeschlossen | verschlüsselt | Fehlschlag | ausgeschlossen |
| SNMP v3 authPriv | ausgeschlossen | verschlüsselt | Klartext | Klartext |
| SNMP v3 authNoPriv | ausgeschlossen | verschlüsselt | Fehlschlag | ausgeschlossen |
| SNMP v3 ohne AuthKein Priv | ausgeschlossen | verschlüsselt | Fehlschlag | ausgeschlossen |

## Switch-Konfiguration für SNMP v3

SNMP v3 mit authPriv ist nicht unbedingt erforderlich, um den Kopiervorgang auszulösen. Da es jedoch mehr Flexibilität und Sicherheit bietet, wird es im Vergleich zu den anderen SNMP-Varianten empfohlen und für die folgenden Beispiele verwendet.

Beispielkonfiguration:

```
snmp-server server

snmp-server engineID local 8000000903f01d2da99341

snmp-server group snmpAdmin v3 priv write Default

encrypted snmp-server user sbscadmin snmpAdmin v3 auth sha
[authentication_password] priv [privacy_password]
```

Mit der obigen Konfiguration kann der Benutzer sbscadmin SNMP v3-Befehle an den Switch senden, um die Dateikopie auszulösen. Der Benutzer sbscadmin ist Mitglied der snmpAdmin-Gruppe, die über vollständige SNMP v3-Schreibberechtigungen für den Switch verfügt.

Beachten Sie, dass der Benutzer sowohl über ein Authentifizierungs- (auth) als auch über ein Datenschutzkennwort (priv) verfügt, d. h., authPriv, und die snmpAdmin-Gruppe ist auf "priv" gesetzt (was ebenfalls Authentifizierung beinhaltet, da Datenschutz ohne diese nicht verwendet werden kann).

## Auslösen der Kopieraufgabe

Im folgenden Beispiel wird der Befehl snmpset verwendet, der den Kopiervorgang auslöst. Es ist lang, da es mehrere Objektwerte setzen muss. Der Befehl wird in einer Zeile eingegeben, aber ein umgekehrter Schrägstrich kann als Escapezeichen verwendet werden, um jedes Element auf einer eigenen Zeile zu trennen, wenn gewünscht. Dies wurde nachfolgend zur Verbesserung der Lesbarkeit durchgeführt. Input wird blau und Output weiß angezeigt.

```
blake@MintBD:~$ snmpset -v 3 -u snmpuser -l authPriv \

-a SHA -A [authentication_password] \

-x AES -X [privacy_password] -m +CISCOSB-COPY-MIB 192.168.111.253 \

rlCopyOptionsRequestedSsdAccess.1 = include-encrypted \

rlCopyRowStatus.1 = createAndGo \

rlCopySourceLocation.1 = local \

rlCopySourceIpAddress.1 = 0.0.0.0 \

rlCopySourceUnitNumber.1 = 1 \

rlCopySourceFileType.1 = runningConfig \
```

```
rlCopyDestinationLocation.1 = tftp \

rlCopyDestinationIpAddress.1 = 192.168.111.18 \

rlCopyDestinationFileName.1 = v3-2.txt \

rlCopyDestinationFileType.1 = backupConfig
```

- An jede OID wird ".1" angehängt, die die Zeile in der Tabelle darstellt, die für die Aufgabe verwendet wird.
- "rlCopyRowStatus.1" wird verwendet, um den Eintrag in die rlCopyTable einzufügen. Sie wird auf "createAndGo" gesetzt, d. h., die Zeile wird erstellt und auf "active" gesetzt, damit sie vom Switch verwendet werden kann.
- Der SSD-Zugriffswert ist auf "include-encrypted" (nur für diese Kopie) festgelegt.
- Die Datei running-config wird auf den TFTP-Server unter der Adresse 192.168.111.18 mit dem Zieldateinamen "v3-2.txt" kopiert.

Nachdem die Kopieraufgabe ausgeführt wurde, wird der Wert von rlCopyOptionsRequestedSsdAccess auf 4 (Standard) zurückgesetzt.

> **Note:**
> Die Verwendung von symbolischen Namen für die Objekte und deren Werte wird durch CISCOSB-COPY-MIB ermöglicht, die in der Datei "CISCOSB-copy.mib", die in den MIB-Dateien auf der Download-Seite für den Switch enthalten ist, ausführlich beschrieben wird.

Die folgende Tabelle entspricht dem symbolischen Namen für jedes Objekt seiner

OID.

| Symbolischer Name | Objektkennung (OID) |
|---|---|
| rlCopyOptionsTable | 1.3.6.1.4.1.9.6.1.101.87.12 |
| rlCopyOptionsRequestedSsdAccess | 1.3.6.1.4.1.9.6.1.101.87.12.1.2 |
| rlCopyTable | 1.3.6.1.4.1.9.6.1.101.87.2 |
| rlCopyRowStatus | 1.3.6.1.4.1.9.6.1.101.87.2.1.17 |
| rlKopieQuellort | 1.3.6.1.4.1.9.6.1.101.87.2.1.3 |
| rlCopySourceIP-Adresse | 1.3.6.1.4.1.9.6.1.101.87.2.1.4 |
| rlKopieQuelleEinheitennummer | 1.3.6.1.4.1.9.6.1.101.87.2.1.5 |
| rlCopySourceFileType | 1.3.6.1.4.1.9.6.1.101.87.2.1.7 |
| rlCopyDestinationLocation | 1.3.6.1.4.1.9.6.1.101.87.2.1.8 |
| rlCopyDestinationIP-Adresse | 1.3.6.1.4.1.9.6.1.101.87.2.1.9 |

| | |
|---|---|
| rlCopyZielDateiname | 1.3.6.1.4.1.9.6.1.101.87.2.1.11 |
| rlCopyDestinationFileType | 1.3.6.1.4.1.9.6.1.101.87.2.1.12 |

Wenn MIB-Dateien nicht verwendet werden, kann die Dateikopie mit den OIDs anstelle der symbolischen Namen ausgelöst werden, obwohl die Ein- und Ausgabe weniger intuitiv ist.

```
blake@MintBD:~$ snmpset -v 3 -u sbscadmin -l authPriv \

-a SHA -A [authentication_password] \

-x AES -X [privacy_password] 192.168.111.253 \

1.3.6.1.4.1.9.6.1.101.87.12.1.2.1 i 1 \

1.3.6.1.4.1.9.6.1.101.87.2.1.17.1 i 4 \

1.3.6.1.4.1.9.6.1.101.87.2.1.3.1 i 1 \

1.3.6.1.4.1.9.6.1.101.87.2.1.4.1 a 0.0.0.0 \

1.3.6.1.4.1.9.6.1.101.87.2.1.5.1 i 1 \

1.3.6.1.4.1.9.6.1.101.87.2.1.7.1 i 2 \

1.3.6.1.4.1.9.6.1.101.87.2.1.8.1 i 3 \

1.3.6.1.4.1.9.6.1.101.87.2.1.9.1 a 192.168.111.18 \

1.3.6.1.4.1.9.6.1.101.87.2.1.11.1 s destination-file.txt \

1.3.6.1.4.1.9.6.1.101.87.2.1.12.1 i 4
```

Ein einfaches "="-Symbol wurde nicht verwendet, um die Werte festzulegen, da der Befehl ohne MIB jeden Objekttyp explizit festlegen muss ("i" für Ganzzahl, "a" für Adresse und "s" für Zeichenfolge). Die Namen für die Werte ("local", "runningConfig" usw.) können ebenfalls nicht verwendet werden, da sie von der MIB definiert werden. Daher müssen die ganzen Zahlen, die diese Optionen darstellen, direkt festgelegt werden.

## Net-SNMP- und Switch-MIB-Dateien

SNMP-Verwaltungstools können für Test- und Fehlerbehebungszwecke hilfreich sein. In diesem Artikel wird der Befehl snmpset verwendet, der im Lieferumfang von Net-SNMP, einer Suite aus freien und Open-Source-SNMP-Tools, enthalten ist.

Um die Switch-MIB-Dateien mit Net-SNMP zu verwenden, stellen Sie zunächst sicher, dass die Net-SNMP-eigenen MIB-Dateien an einem Speicherort abgelegt werden, an dem Net-SNMP nach ihnen sucht, z. B. $HOME/.snmp/mibs. Ohne die installierten Net-SNMP MIB-Dateien funktionieren die Switch-MIBs nicht ordnungsgemäß.

Die Switch-MIB-Dateien können extrahiert und am gleichen Speicherort wie die MIB-Dateien von Net-SNMP abgelegt werden. Um Kompatibilitätsprobleme zu vermeiden, sollten Sie jedoch die Net-SNMP-Versionen von nicht überschreiben, die sich zwischen den beiden Gruppen überschneiden.

Sobald sich alle MIB-Dateien an einem geeigneten Speicherort befinden, können die relevanten MIB(s) mit dem Argument "-m" mit dem gewünschten Befehl aufgerufen werden.

Beispiele:

```
snmpget -v 3 -u snmpuser -l authPriv \

-a SHA -A [authentication_password] \

-x AES -X [privacy_password] \

                    192.168.111.253 rlCopyOptionsRequestedSsdAccess.1
```

> **Note:**
> "CISCOSB-COPY-MIB" ist der Name der MIB selbst und nicht die Datei, die sie beschreibt, nämlich CISCOSB-copy.mib.

Weitere Informationen zur Verwendung der Net-SNMP-Tools finden Sie in der Dokumentation und den Tutorials, die auf der Net-SNMP-Website verfügbar sind.

## Schlussfolgerung

Nun wissen Sie, wie Sie das Kopieren der Konfigurationsdateien von einem Cisco Business Switch über SNMP auf einen TFTP-Server auslösen können.

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.