

# Konfigurationsbeispiel für Telnet-, Konsolen- und AUX-Port-Kennwörter auf Cisco Routern

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Konfigurieren von Kennwörtern auf der Leitung](#)

[Konfigurationsverfahren](#)

[Überprüfen der Konfiguration](#)

[Fehlerbehebung bei Anmeldefehlern](#)

[Lokale benutzerspezifische Kennwörter konfigurieren](#)

[Konfigurationsverfahren](#)

[Überprüfen der Konfiguration](#)

[Fehlerbehebung bei benutzerspezifischem Kennwortfehler](#)

[AUX-Leitungskennwort konfigurieren](#)

[Konfigurationsverfahren](#)

[Konfiguration überprüfen](#)

[Konfigurieren der AAA-Authentifizierung für die Anmeldung](#)

[Konfigurationsverfahren](#)

[Überprüfen der Konfiguration](#)

[Fehlerbehebung bei AAA-Anmeldefehlern](#)

[Zugehörige Informationen](#)

## Einleitung

Dieses Dokument enthält Beispielkonfigurationen für die Konfiguration des Kennwortschutzes für eingehende EXEC-Verbindungen mit dem Router.

## Voraussetzungen

### Anforderungen

Um die in diesem Dokument beschriebenen Aufgaben ausführen zu können, müssen Sie über einen privilegierten EXEC-Zugriff auf die Befehlszeilenschnittstelle (CLI) des Routers verfügen. Informationen zur Verwendung der Befehlszeile und zum Verständnis der Befehlsmodi finden Sie unter [Verwenden der Cisco IOS-Befehlszeilenschnittstelle](#).

Anweisungen zum Anschließen einer Konsole an den Router finden Sie in der Dokumentation des Routers oder in der [Online-Dokumentation](#) für Ihr Gerät.

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Router der Serie 2509
- Cisco IOS® Software Version 12.2(19)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps von Cisco zu Konventionen).

## Hintergrundinformationen

Die Verwendung von Kennwortschutz zur Kontrolle oder Einschränkung des Zugriffs auf die Befehlszeilenschnittstelle (CLI) Ihres Routers ist eines der grundlegenden Elemente eines allgemeinen Sicherheitsplans.

Der Schutz des Routers vor nicht autorisiertem Remote-Zugriff, in der Regel Telnet, ist die häufigste Sicherheitsmaßnahme, die konfiguriert werden muss. Der Schutz des Routers vor nicht autorisiertem lokalen Zugriff kann jedoch nicht übersehen werden.

**Hinweis:** Der Kennwortschutz ist nur einer der vielen Schritte, die Sie in einem effektiven und detaillierten Netzwerk-Sicherheitsschema durchführen sollten. Firewalls, Zugriffslisten und die Kontrolle des physischen Zugriffs auf die Geräte sind weitere Elemente, die bei der Implementierung Ihres Sicherheitsplans berücksichtigt werden müssen.

Die Befehlszeile (oder EXEC, der Zugriff auf einen Router) kann auf verschiedene Weise erfolgen, aber in allen Fällen erfolgt die eingehende Verbindung mit dem Router über eine TTY-Leitung. Es gibt vier Haupttypen von TTY-Zeilen, wie in diesem Beispiel die **Ausgabe** der **angezeigten Zeile** gezeigt:

```
2509#show line
```

Tty	Typ	Tx/Rx	A	Modem	Roty	AccO	AccI	Uses	Noise	Overruns	Int
*	0	<b>CTY</b>	-	-	-	-	-	0	0	0/0	-
	1	<b>TTY</b>	9600/9600	-	-	-	-	0	0	0/0	-
	2	<b>TTY</b>	9600/9600	-	-	-	-	0	0	0/0	-
	3	<b>TTY</b>	9600/9600	-	-	-	-	0	0	0/0	-
	4	<b>TTY</b>	9600/9600	-	-	-	-	0	0	0/0	-
	5	<b>TTY</b>	9600/9600	-	-	-	-	0	0	0/0	-
	6	<b>TTY</b>	9600/9600	-	-	-	-	0	0	0/0	-
	7	<b>TTY</b>	9600/9600	-	-	-	-	0	0	0/0	-
	8	<b>TTY</b>	9600/9600	-	-	-	-	0	0	0/0	-
	9	<b>AUX</b>	9600/9600	-	-	-	-	0	0	0/0	-
	10	<b>VTY</b>		-	-	-	-	0	0	0/0	-
	11	<b>VTY</b>		-	-	-	-	0	0	0/0	-
	12	<b>VTY</b>		-	-	-	-	0	0	0/0	-

13	<b>VTY</b>	-	-	-	-	-	0	0	0/0	-
14	<b>VTY</b>	-	-	-	-	-	0	0	0/0	-

2509#

Der **CTY**-Leitungstyp ist der Konsolenport. Auf jedem Router wird er in der Router-Konfiguration als **line con 0** und in der Ausgabe des Befehls **show line** als **cty** angezeigt. Der Konsolenport wird hauptsächlich für den Zugriff auf das lokale System über einen Konsolenterminal verwendet.

Bei den **TTY**-Leitungen handelt es sich um asynchrone Leitungen für ein- und ausgehende Modem- und Terminalverbindungen, die in einer Router- oder Zugriffsserver-Konfiguration als **Zeile x** angezeigt werden. Die spezifischen Leitungsnummern sind abhängig von der Hardware, die auf dem Router oder Zugriffsserver installiert ist.

Die **AUX**-Leitung ist der Hilfsport, der in der Konfiguration als **Zeile aux 0** angesehen wird.

Die **VTY**-Leitungen sind die virtuellen Terminallinien des Routers, die ausschließlich zur Steuerung von eingehenden Telnet-Verbindungen verwendet werden. Sie sind virtuell, da sie eine Funktion von Software sind - ihnen ist keine Hardware zugeordnet. Sie werden in der Konfiguration als **Zeile vty 0 4** angezeigt.

Jeder dieser Leitungsarten kann mit Kennwortschutz konfiguriert werden. Leitungen können so konfiguriert werden, dass sie ein Kennwort für alle Benutzer oder für benutzerdefinierte Kennwörter verwenden. Benutzerspezifische Kennwörter können lokal auf dem Router konfiguriert werden, oder Sie können einen Authentifizierungsserver verwenden, um Authentifizierung bereitzustellen.

Es ist nicht verboten, verschiedene Posten mit verschiedenen Arten von Kennwortschutz zu konfigurieren. Tatsächlich ist es üblich, Router mit einem einzigen Kennwort für die Konsole und benutzerspezifische Kennwörter für andere eingehende Verbindungen zu sehen.

Im Folgenden finden Sie ein Beispiel für die Ausgabe des Routers über den Befehl **show running-config**:

```
2509#show running-config
Building configuration...
```

```
Current configuration : 655 bytes
```

```
!
version 12.2
.
.
.
!--- Configuration edited for brevity line con 0 line 1 8 line aux 0 line vty 0 4 ! end
```

## Konfigurieren von Kennwörtern auf der Leitung

Um ein Kennwort für eine Zeile anzugeben, verwenden Sie den Befehl **password** im Leitungskonfigurationsmodus. Um die Kennwortprüfung bei der Anmeldung zu aktivieren, verwenden Sie den Befehl **login** im Leitungskonfigurationsmodus.

## Konfigurationsverfahren

In diesem Beispiel wird ein Kennwort für alle Benutzer konfiguriert, die versuchen, die Konsole zu verwenden.

1. Geben Sie an der Eingabeaufforderung für privilegierten EXEC (oder "enable") in den Konfigurationsmodus ein, und wechseln Sie mit den folgenden Befehlen in den Leitungskonfigurationsmodus. Beachten Sie, dass sich die Eingabeaufforderung ändert, um den aktuellen Modus wiederzugeben.

```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#line con 0
router(config-line)#
```

2. Konfigurieren Sie das Kennwort, und aktivieren Sie die Kennwortprüfung bei der Anmeldung.

```
router(config-line)#password letmein
router(config-line)#login
```

3. Beenden Sie den Konfigurationsmodus.

```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```

**Hinweis:** Speichern Sie die Konfigurationsänderungen nicht in **line con 0**, bevor Sie sich anmelden können.

**Hinweis:** Bei der Leitungskonsolenkonfiguration ist **login** ein erforderlicher Konfigurationsbefehl, um die Kennwortprüfung bei der Anmeldung zu aktivieren. Die Konsolenthifizierung erfordert sowohl das **Kennwort** als auch die **Anmeldebefehle**.

## Überprüfen der Konfiguration

Überprüfen Sie die Konfiguration des Routers, um sicherzustellen, dass die Befehle korrekt eingegeben wurden:

- **show running-config** - Zeigt die aktuelle Konfiguration des Routers an.

```
router#show running-config
Building configuration...
...
!--- Lines omitted for brevity ! line con 0 password letmein
login
line 1 8
line aux 0
line vty 0 4
!
end
```

Um die Konfiguration zu testen, melden Sie sich von der Konsole ab, und melden Sie sich erneut mit dem konfigurierten Kennwort für den Zugriff auf den Router an:

```
router#exit

router con0 is now available

Press RETURN to get started.

User Access Verification
Password:
!--- Password entered here is not displayed by the router router>
```

**Hinweis:** Bevor Sie diesen Test durchführen, stellen Sie sicher, dass Sie eine alternative Verbindung zum Router haben, z. B. Telnet oder Einwahlverbindung, falls ein Problem bei der Anmeldung beim Router auftritt.

## Fehlerbehebung bei Anmeldefehlern

Wenn Sie sich nicht wieder beim Router anmelden können und die Konfiguration nicht gespeichert wurde, werden alle vorgenommenen Konfigurationsänderungen durch das Neuladen des Routers eliminiert.

Wenn die Konfigurationsänderungen gespeichert wurden und Sie sich nicht beim Router anmelden können, müssen Sie eine Kennwortwiederherstellung durchführen. Unter [Verfahren zur Kennwortwiederherstellung](#) finden Sie Anweisungen für Ihre spezielle Plattform.

## Lokale benutzerspezifische Kennwörter konfigurieren

Um ein username-basiertes Authentifizierungssystem einzurichten, verwenden Sie den Befehl **username** im globalen Konfigurationsmodus. Um die Kennwortprüfung bei der Anmeldung zu aktivieren, verwenden Sie den Befehl **login local** in line configuration mode.

### Konfigurationsverfahren

In diesem Beispiel werden Kennwörter für Benutzer konfiguriert, die versuchen, mithilfe von Telnet eine Verbindung zum Router auf den VTY-Leitungen herzustellen.

1. Geben Sie an der Eingabeaufforderung für privilegiertes EXEC (oder "enable") in den Konfigurationsmodus ein, und geben Sie Kombinationen aus Benutzername und Kennwort ein, einer für jeden Benutzer, dem der Zugriff auf den Router gestattet werden soll:

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#username russ password montecito
router(config)#username cindy password belgium
router(config)#username mike password rottweiler
```

2. Wechseln Sie mithilfe der folgenden Befehle in den Leitungskonfigurationsmodus. Beachten Sie, dass sich die Eingabeaufforderung ändert, um den aktuellen Modus wiederzugeben.

```
router(config)#line vty 0 4
router(config-line)#
```

3. Konfigurieren Sie die Kennwortprüfung bei der Anmeldung.

```
router(config-line)#login local
```

4. Beenden Sie den Konfigurationsmodus.

```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```

**Hinweis:** Um Auto Telnet zu deaktivieren, wenn Sie einen Namen in der CLI eingeben, müssen Sie **keine bevorzugte Protokollierung** für die verwendete Leitung konfigurieren. Obwohl **transport preferred none** dieselbe Ausgabe bereitstellt, deaktiviert es auch Auto Telnet für den definierten Host, der mit dem **ip host**-Befehl konfiguriert ist. Dies ist anders als der Befehl **no logging preferred**, der ihn für nicht definierte Hosts stoppt und für die definierten Hosts funktioniert.

### Überprüfen der Konfiguration

Überprüfen Sie die Konfiguration des Routers, um sicherzustellen, dass die Befehle korrekt eingegeben wurden:

- **show running-config** - Zeigt die aktuelle Konfiguration des Routers an.

```
router#show running-config
Building configuration...
!
!--- Lines omitted for brevity ! username russ password 0 montecito
username cindy password 0 belgium
username mike password 0 rottweiler
!
!--- Lines omitted for brevity ! line con 0 line 1 8 line aux 0 line vty 0 4 login local
!
end
```

Um diese Konfiguration zu testen, muss eine Telnet-Verbindung zum Router hergestellt werden. Dies kann über eine Verbindung von einem anderen Host im Netzwerk erfolgen, Sie können jedoch auch vom Router selbst testen, indem Sie eine Telnet-Verbindung mit der IP-Adresse einer beliebigen Schnittstelle auf dem Router herstellen, die sich im Ein-/Ausschaltzustand befindet, wie in der Ausgabe des Befehls **show interfaces** zu sehen ist. Im Folgenden finden Sie eine Beispielausgabe, wenn die Adresse von **Interface Ethernet 0 10.1.1.1** betrug:

```
router#telnet 10.1.1.1
Trying 10.1.1.1 ... Open
```

```
User Access Verification
```

```
Username: mike
Password:
```

```
!--- Password entered here is not displayed by the router router
```

## Fehlerbehebung bei benutzerspezifischem Kennwortfehler

Bei Benutzernamen und Passwörtern wird die Groß- und Kleinschreibung beachtet. Benutzer, die sich mit einem Benutzernamen oder einem Kennwort anmelden möchten, der nicht korrekt eingegeben wurde, werden abgelehnt.

Wenn Benutzer sich nicht mit ihren spezifischen Kennwörtern beim Router anmelden können, müssen Sie den Benutzernamen und das Kennwort auf dem Router neu konfigurieren.

## AUX-Leitungskennwort konfigurieren

Um ein Kennwort für die AUX-Leitung anzugeben, geben Sie den Befehl **password** im Leitungskonfigurationsmodus ein. Um die Kennwortprüfung bei der Anmeldung zu aktivieren, geben Sie den Befehl **login** im Leitungskonfigurationsmodus aus.

## Konfigurationsverfahren

In diesem Beispiel wird ein Kennwort für alle Benutzer konfiguriert, die versuchen, den AUX-Port zu verwenden.

1. Geben Sie den Befehl **show line** ein, um die vom AUX-Port verwendete Leitung zu überprüfen.

```
R1#show line
```

Tty	Typ	Tx/Rx	A	Modem	Roty	AccO	AccI	Uses	Noise	Overruns	Int	
*	0	CTY		-	-	-	-	-	0	0	0/0	-
	65	AUX	9600/9600	-	-	-	-	0	1	0/0		-
	66	VTY		-	-	-	-	-	0	0	0/0	-
	67	VTY		-	-	-	-	-	0	0	0/0	-

2. In diesem Beispiel befindet sich der AUX-Port in Zeile 65. Führen Sie die folgenden Befehle aus, um die AUX-Leitung des Routers zu konfigurieren:

```
R1# conf t
R1(config)# line 65
R1(config-line)#modem inout
R1(config-line)#speed 115200
R1(config-line)#transport input all
R1(config-line)#flowcontrol hardware
R1(config-line)#login
R1(config-line)#password cisco
R1(config-line)#end
R1#
```

## Konfiguration überprüfen

Überprüfen Sie die Konfiguration des Routers, um sicherzustellen, dass die Befehle korrekt eingegeben wurden:

- Der Befehl **show running-config** zeigt die aktuelle Konfiguration des Routers an:

```
R1#show running-config
Building configuration...
!
!--- Lines omitted for brevity. line aux 0
password cisco
login
modem InOut
transport input all
speed 115200
flowcontrol hardware

!--- Lines omitted for brevity. ! end
```

## Konfigurieren der AAA-Authentifizierung für die Anmeldung

Um die Authentifizierung, Autorisierung und Accounting (AAA)-Authentifizierung für Anmeldungen zu aktivieren, verwenden Sie den Befehl **login authentication** im Leitungskonfigurationsmodus. AAA-Services müssen ebenfalls konfiguriert werden.

### Konfigurationsverfahren

In diesem Beispiel ist der Router so konfiguriert, dass Benutzer-Passwörter von einem TACACS+-Server abrufen, wenn Benutzer versuchen, eine Verbindung zum Router herzustellen.

**Hinweis:** Die Konfiguration des Routers für die Verwendung anderer AAA-Servertypen (z. B. RADIUS) ist ähnlich. Weitere Informationen finden Sie unter [Konfigurieren der Authentifizierung](#).

**Hinweis:** Dieses Dokument behandelt nicht die Konfiguration des AAA-Servers selbst.

1. Geben Sie an der Eingabeaufforderung für den privilegierten EXEC (oder "enable") in den

Konfigurationsmodus ein, und geben Sie die Befehle ein, um den Router für die Verwendung der AAA-Dienste für die Authentifizierung zu konfigurieren:

```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#aaa new-model
router(config)#aaa authentication login my-auth-list tacacs+
router(config)#tacacs-server host 192.168.1.101
router(config)#tacacs-server key letmein
```

2. Wechseln Sie mithilfe der folgenden Befehle in den Leitungskonfigurationsmodus. Beachten Sie, dass sich die Eingabeaufforderung ändert, um den aktuellen Modus wiederzugeben.

```
router(config)#line 1 8
router(config-line)#
```

3. Konfigurieren Sie die Kennwortprüfung bei der Anmeldung.

```
router(config-line)#login authentication my-auth-list
```

4. Beenden Sie den Konfigurationsmodus.

```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```

## Überprüfen der Konfiguration

Überprüfen Sie die Konfiguration des Routers, um sicherzustellen, dass die Befehle korrekt eingegeben wurden:

- **show running-config** - Zeigt die aktuelle Konfiguration des Routers an.

```
router#write terminal
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
aaa new-model
aaa authentication login my-auth-list tacacs+
!
!--- Lines omitted for brevity ... ! tacacs-server host 192.168.1.101
tacacs-server key letmein
!
line con 0
line 1 8
  login authentication my-auth-list
line aux 0
line vty 0 4
!
end
```

Um diese Konfiguration zu testen, muss eine eingehende oder ausgehende Verbindung zur Leitung hergestellt werden. Weitere Informationen zum Konfigurieren asynchroner Leitungen für Modemverbindungen finden Sie im [Modem - Router Connection Guide](#).

Alternativ können Sie eine oder mehrere VTY-Zeilen konfigurieren, um eine AAA-Authentifizierung durchzuführen und die Tests durchzuführen.



## Fehlerbehebung bei AAA-Anmeldefehlern

Bevor Sie **Debugbefehle** ausgeben, [sollten Sie unter Wichtige Informationen über Debug-Befehle](#) nachlesen.

Um eine Fehlerbehebung bei einem fehlgeschlagenen Anmeldeversuch durchzuführen, verwenden Sie den für die Konfiguration passenden **debug**-Befehl:

- [debuggen aaa authentication](#)
- [Debug-Radius](#)
- [Debug-Kerberos](#)

## Zugehörige Informationen

- [Cisco IOS-Debug-Befehlsreferenz](#)
- [Technischer Support – Cisco Systems](#)