# Häufig gestellte Fragen zur Content-Sicherheit: Wie greifen Sie auf die CLI einer Content Security Appliance zu?

## Inhalt



## Einführung

In diesem Dokument wird beschrieben, wie Sie über einen Telnet- oder Secure Shell (SSH)-Client auf einer Cisco Content Security Appliance auf die CLI zugreifen.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco E-Mail Security Appliance (ESA)
- Cisco Web Security Appliance (WSA)
- Cisco Security Management Appliance (SMA)
- AsyncOS

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ESA AsyncOS, alle Versionen
- Cisco WSA AsyncOS, alle Versionen
- Cisco SMA-Versionen AsyncOS, alle Versionen

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie

die potenziellen Auswirkungen eines Befehls verstehen.

> **Hinweis**: Dieses Dokument bezieht sich auf Software, die nicht von Cisco verwaltet oder unterstützt wird. Die Informationen werden Ihnen zu Ihrer Zufriedenheit zur Verfügung gestellt. Wenden Sie sich für weitere Unterstützung an den Softwareanbieter.

## Wie greifen Sie auf die CLI einer Content Security Appliance zu?

Sie können über einen Telnet-Client oder einen SSH-Client auf die CLI Ihrer Appliance zugreifen. Das Telnet-Protokoll ist jedoch unverschlüsselt, sodass Ihre Anmeldeinformationen einfacher gestohlen werden können, wenn Sie sich über Telnet bei Ihrer Appliance anmelden.

Cisco empfiehlt, dass alle Produktionsmaschinen einen SSH-Client verwenden. Darüber hinaus ist der Standard-Microsoft Windows Telnet-Client schwer zu verwenden. Telnet wird standardmäßig auf dem Management-Port konfiguriert.

Gehen Sie wie folgt vor, um Telnet zu deaktivieren:

1. Melden Sie sich bei der Web-GUI an.
2. Navigieren Sie zu **Netzwerk > IP-Schnittstellen**.
3. Klicken Sie auf den Namen der Schnittstelle, die Sie bearbeiten möchten.
4. Deaktivieren Sie das Kontrollkästchen **Telnet** im Feld Dienste.

Gehen Sie wie folgt vor, um über SSH (Port 22) auf Ihre Appliance zuzugreifen:

1. Installieren Sie einen SSH-Client in Microsoft Windows, z. B. PuTTY.
2. Starten Sie den SSH-Client:

   Fügen Sie die Hostinformationen für Ihre Appliance hinzu (z. B. **c650.example.com**).

   Klicken Sie auf **Laden**.

   Geben Sie Ihren Benutzernamen ein.

   Geben Sie Ihr Kennwort ein.
3. Öffnen Sie eine Eingabeaufforderung mit ***nix**.
4. Geben Sie den Befehl **$ ssh exampleC650.com ein**.
5. Wenn Sie einen anderen Benutzer angeben müssen, geben Sie den Befehl **$ ssh <user>@exampleC650.com ein**. Wenn der Benutzername **admin** ist, geben Sie den Befehl **$ ssh admin@C650.example.com ein**.

Gehen Sie wie folgt vor, um über Telnet auf Ihre Appliance zuzugreifen:

> **Hinweis**: Cisco empfiehlt, einen SSH-Client für den Zugriff zu verwenden. Die Anwendung von Telnet wird nicht empfohlen.

1. Öffnen Sie eine Eingabeaufforderung.
2. Geben Sie den Befehl **telnet c650.example.com ein**.
3. Geben Sie Ihren Benutzernamen ein.
4. Geben Sie Ihr Kennwort ein.