

# CLI (Read only Command Line Interface) für CUCM konfigurieren

## Inhalt

[Einführung:](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Funktionsweise in 11.5](#)

[Konfigurieren](#)

[Beispiele:](#)

[Befehl mit Privilege 0](#)

## Einführung:

Dieses Dokument beschreibt die neue Read-only-CLI-Funktion, die in Version 11.5 von Cisco Unified Communications Manager (CUCM) eingeführt wurde.

Unterstützt von Manjunath Junnur, Cisco TAC Engineer, herausgegeben von Levi Thomas.

## Voraussetzungen

## Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco Unified Communications Manager Version 11.5

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.

## Hintergrundinformationen

In der Kundenumgebung ist häufig die Möglichkeit für Benutzer mit eingeschränktem Zugriff auf CLI-Befehle erforderlich.

In dieser Version wurde die Funktion für schreibgeschützte Berechtigungen für CLI integriert.

CUCM- und IM&P-Administratoren können Benutzerkonten und schreibgeschützten Zugriff auf die Befehlszeilenschnittstelle (CLI) bereitstellen, sodass vorhandene Einstellungsinformationen zwar sichtbar, aber nicht änderbar sind.

**Hinweis:** Befehle für Schreibvorgänge werden für schreibgeschützte Benutzer von Benutzerkonten abgelehnt.

# Funktionsweise in 11.5

- Derzeit erstellt der Befehl **set account name** in der aktuellen CLI-Architektur zwei Benutzertypen.

1. **Level-0-Berechtigung** (schreibgeschützter/normaler Benutzer)

2. **Level-1-Berechtigung** (berechtigter Benutzer)

**Schreibgeschützter Benutzer:** Schreibgeschützte Benutzer können nur auf schreibgeschützte Befehle zugreifen, z. B. (Anzeigen, Status); Sie können nicht auf Einstellungen zugreifen, Befehle löschen oder Einstellungen aktivieren/deaktivieren. Wenn ein Befehl zum schreibgeschützten Befehl wird, lautet der Wert in der XML-Konfigurationsdatei der CLI "priv" 0 und kann von schreibgeschützten Benutzern aufgerufen werden.

**Privilegierter Benutzer:** Gemäß dem Design können privilegierte Benutzer auch auf schreibgeschützte Befehle und Schreibbefehle zugreifen. Wenn ein Befehl in der CLI-Konfigurationsdatei den Wert "priv" 1 hat, können diese Befehle nur von privilegierten Benutzern aufgerufen werden. Berechtigungen von Benutzern können auf Befehle mit dem Wert 0 und 1 zugreifen.

**Administrator-Benutzer:** Der Administrator-Benutzer hat Zugriff auf alle Befehle. Der Admin-Benutzer hat 4. In der CLI-Konfigurationsdatei Wenn der Wert "priv" 4 lautet, greift der Administrator auf diese Befehle zu. Administratorbenutzer können auch auf Befehle der 4-, 1- und 0-Ebene zugreifen.

## Konfigurieren

Um das schreibgeschützte Benutzerkonto zu erstellen, melden Sie sich bei der CLI an, und verwenden Sie den Befehl.

admin:Kontonamen <Geben Sie einen beliebigen Namen ein>

Die Berechtigungsstufen sind:

**Normal - Stufe 0**

Erweitert - Stufe 1

Wählen Sie 0 für den schreibgeschützten Access-Benutzer aus.

### Konfigurieren des Kennworts für den Benutzer

Geben Sie das Kennwort ein:\*\*\*\*\*

zur Bestätigung erneut eingeben:\*\*\*\*\*

Screenshot für dasselbe Beispiel:

```
admin:set account name ciscotac

Privilege Levels are:
  Ordinary - Level 0
  Advanced - Level 1

Please enter the privilege level :0 ←
Please enter the password :*****
re-enter to confirm :*****
Account successfully created
```

## Beispiele:

Beispiel 1: Melden Sie sich mit schreibgeschützten Benutzeranmeldeinformationen an, und versuchen Sie, die DB-Replikation zu beenden.

```
admin:utils dbreplication stop all
Executed command unsuccessfully ←
No valid command entered
admin: █
```

Beispiel 2: Usi sql-Abfrage, um eine Region zu löschen.

```
[admin:run sql delete from region where region ="91b78ae6-6e6b-f9fd-cd1d-380a1b188034"
No DELETE permission for region. ←
```

Beispiel 3: Schreibgeschützte Benutzer können jeden Show-Befehl verwenden.

```
[admin:show version active ←
Active Master Version: 11.5.0.99838-4
Active Version Installed Software Options:
No Installed Software Options Found.
```

Beispiel 4: Melden Sie sich bei der grafischen Benutzeroberfläche (GUI) Operating System (OS) Admin mit Read only User an, und Sie können sehen, dass auf jeder Registerkarte kein Schreibzugriff vorhanden ist. Wenn Sie ein Zertifikat öffnen, enthält es die Details, es gibt jedoch keine Optionen zum Löschen oder Neugenerieren.

## Certificate Details for publisher, CallManager

### Status



Status: Ready

### Certificate Settings

File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

### Certificate File Data

```
[
Version: V3
Serial Number: 45BA6326E241B27DCA57D66E80F61F33
SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: L=Bangalore, ST=Karnataka, CN=publisher, OU=Cisco, O=Cisco,
C=IN
Validity From: Fri May 27 13:00:14 IST 2016
          To:   Wed May 26 13:00:13 IST 2021
Subject Name: L=Bangalore, ST=Karnataka, CN=publisher, OU=Cisco,
O=Cisco, C=IN
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100d634eb2a09e5ac0e91015ece7696040fa5f20baae7c4010cf0
863303e46b8d6fd73a8b5481d4cefd89ade3f5ede53dae3c89aaa7df080263d4de52a
f2dfcfec961946239d00bb7f4d13f76a777b93e57cdf5486ea2ad205b55fb0be6604a2
```

## Befehl mit Privilege 0

Beispiel für Befehle mit der Berechtigung 0

- Anzeigestatus
- Anzeigeprozess mit der meisten CPU
- utils dbreplication runtime state
- show network eth0
- utils Service-Liste