

# 為CUCM配置只讀命令列介面(CLI)

## 目錄

[簡介:](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[在11.5中如何工作](#)

[設定](#)

[範例:](#)

[具有許可權0的命令](#)

## 簡介:

本檔案介紹Cisco Unified Communications Manager(CUCM)版本11.5中引入的新只讀CLI功能。

作者：思科TAC工程師Manjunath Junnur，編輯者：Levi Thomas。

## 必要條件

## 需求

本文件沒有特定需求。

## 採用元件

本檔案中的資訊是根據以下軟體版本：

- 思科整合通訊管理員版本11.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

通常，客戶環境需要具有有限的CLI命令訪問能力。

在此版本中，它包含了CLI的只讀許可權功能。

CUCM和IM&P管理員可以在命令列介面(CLI)上提供使用者帳戶和只讀許可權，因此現有設定資訊可見但不可更改。

**附註：**只讀許可權帳戶使用者拒絕寫入操作命令。

## 在11.5中如何工作

- 目前，在當前CLI架構中，**set account name**命令會建立兩種型別的使用者。

1. **0級許可權**（只讀/普通使用者）

## 2. 1級許可權 (特權使用者)

只讀使用者：只讀使用者，只能訪問只讀命令，如(show, status);它們不能訪問set、delete命令或啟用/禁用設定。如果任何命令變為只讀命令，則在CLI配置xml檔案「priv」中，值為0，且只讀使用者可訪問該值。

特權使用者：根據設計，特權使用者可以訪問只讀命令和寫命令。如果命令列在cli配置檔案中具有「priv」值1，則這些命令只能由特權使用者訪問。特權使用者可以訪問具有priv值0和1的命令

管理員使用者：Admin使用者有權訪問所有命令，Admin使用者級別為4。在cli配置檔案中，如果「priv」值為4，則admin使用者將訪問這些命令。管理員使用者還可以訪問priv value 4、1、0級命令

## 設定

要建立只讀使用者帳戶，請登入CLI並使用命令。

```
admin:set account name <input any name>
```

許可權級別為：

— 0  
高級 — 1級

選擇0作為只讀訪問使用者。

請輸入密碼：\*\*\*\*\*  
重新輸入以確認：\*\*\*\*\*

螢幕截圖：

```
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
```

## 範例：

範例 1：使用只讀使用者憑據登入，並嘗試停止資料庫複製

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

範例 2：使用sql查詢刪除區域。

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

範例 3:只讀使用者，可以使用任何Show命令。

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

範例 4:使用只讀使用者登入圖形使用者介面(GUI)作業系統(OS)管理員，您可以看到在任何頁籤上都沒有寫訪問許可權。如果開啟任何證書，則其中包含詳細資訊，但沒有可刪除或重新生成的選項。

### 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
```

## 具有許可權0的命令

許可權為0的命令示例

- 顯示狀態

- show process using-most cpu
- 實用工具dbremote runtimestate
- show network eth0
- utils service list