

# Configure Read only Command Line Interface (CLI) for CUCM

## Contents

[Introduction:](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[How it works in 11.5](#)

[Configure](#)

[Examples :](#)

[Command with Privilege 0](#)

## Introduction:

This document describes the new Read only CLI feature introduced in Cisco Unified Communications Manager (CUCM) version 11.5.

Contributed by Manjunath Junnur, Cisco TAC Engineer, Edited by Levi Thomas.

## Prerequisites

## Requirements

There are no specific requirements for this document.

## Components Used

The information in this document is based on these software versions:

- Cisco Unified Communications Manager version 11.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

Often Customers environment requires the ability for users with limited CLI commands access.

On this version, it was included the read only permission feature for CLI.

CUCM and IM&P Administrators can provide users accounts, Read-Only privileges access on the Command Line Interface (CLI), so existing settings information are visible but not changeable.

**Note:** Commands for write operations are denied for Read-Only Privilege Account users.

## How it works in 11.5

- At present in current CLI architecture the **set account name** command, creates two type of users.

1. **Level 0 privilege** (Read-only/Ordinary user)

2. **Level 1 privilege** (Privileged user)

**Read-only user:** Read-only users, can access only read only commands like(show, status); they cannot access set, delete commands or enable/disable settings. If any command become read-only command, in the CLI configuration xml file "priv", value is 0 and that can be accessed by read-only users.

**Privileged user:** As per design, privileged users can access read only commands and write commands as well. If any command, in cli configuration file has "priv" value 1, those commands can be access by privileged users only. Privileged users can access command with priv value 0 and 1

**Admin user :** Admin user have access for all the commands, The level of Admin user is 4. In the cli configuration file If "priv" value is 4 admin user will access those commands. Admin user can access priv value 4,1,0 level commands as well

## Configure

In order to create the Read only user account, Log in CLI and use the command.

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

Privilege Levels are:

**Ordinary - Level 0**

Advanced - Level 1

Select 0 for the read only Access user.

**Configure password for the user**

Please enter the password :\*\*\*\*\*

re-enter to confirm :\*\*\*\*\*

Screenshot for the same:

```
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
```

## Examples :

Example 1 : Log in with Read only user credentials and try the DB replication stop

```
admin:utils dbreplication stop all
```

```
Executed command unsuccessfully ←
```

```
No valid command entered
```

```
admin: █
```

Example 2 : Use sql query in order to delete a region .

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

Example 3 : Read only users, can use any Show command.


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

Example 4 : Log in the Graphical User Interface (GUI) Operating System (OS) Admin with read only User and you can observe there are no write access on any tab. If you open any certificate, it contains the details however there are no options to delete or regenerate.

### 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
```

## Command with Privilege 0

Example of commands with privilege 0

- show status
- show process using-most cpu
- utils dbreplication runtimestate
- show network eth0
- utils service list