

Unable to Login to the Cisco DCM GUI after Upgrade to a Version Higher than 16.10

Contents

[Introduction](#)

[Background Information](#)

[Problem](#)

[Root Cause](#)

[Solution](#)

Introduction

This document describes the solution to the problem that arises after a software is upgraded from a version lower than 16.10 to a higher version, where you might not be able to log in to Digital Content Manager (DCM) GUI anymore.

Background Information

The DCM is accessible with the use of GUI. In order to protect the device configuration from unauthorised access by users, DCM has a login/password feature. You can set up its security and define the security accounts with unique username and password. Particular rights to users can be given when you add security accounts to security groups. Access can be defined by security accounts to the DCM GUI or accounts can be defined to access the DCM by external IP services. View of a question related to Administrators. Administrators - GUI accounts with full access. Usually the GUI accounts that belong to the administrators security group and OS accounts must be created at the time of the first initial security DCM setup.

Problem

You cannot log in to the admin account name after you upgrade from v16.10 to 20.10.

It might seem that the authentication goes ahead and the main page gets loaded, however, after a few seconds you are redirected again to the log in page with the

URL; https://IPaddress/login?came_from=AdminLoggedOut.

You notice that you are only able to log in to the GUI via ROSA. When you double click on the **DCM** in ROSA, it opens up the browser and the authentication goes ahead correctly.

New GUI accounts have been added after the upgrade (via the ROSA access), and with this new GUI account, customers are able to login, but not with an account that was defined before the upgrade.


Root Cause

In older versions it was possible to add an admin/admin account as a GUI account. Checked version that allows such account creation is v11.10.07.


But in newer versions, v15.10.00 and higher, it is impossible. GUI Account - admin creation process is interrupted with a warning message as shown in this image.

Local Remote

Reload Apply ?

 We've encountered a problem with your submission.
Please correct the fields labeled below.
User Name - The user name must be unique (regardless of the case).

GUI Accounts ?

	Account Name	Security Group	Change Password
<input type="checkbox"/>	Administrator 	Administrators (Full Control) ▼	<input type="checkbox"/>
<input type="checkbox"/>	Guest	Guests (Read-Only) ▼	<input type="checkbox"/>
<input type="checkbox"/>	Temporary	Administrators (Full Control) ▼	<input type="checkbox"/>

Remove Checked Items

Add New GUI Account ?

User Name *

Security Group

Password

Re-enter Password

Ignore Password Policy

Add Account

The error occurs because admin/admin account is the default account for the first login, that is used usually at the time of the initial IP configuration procedure.

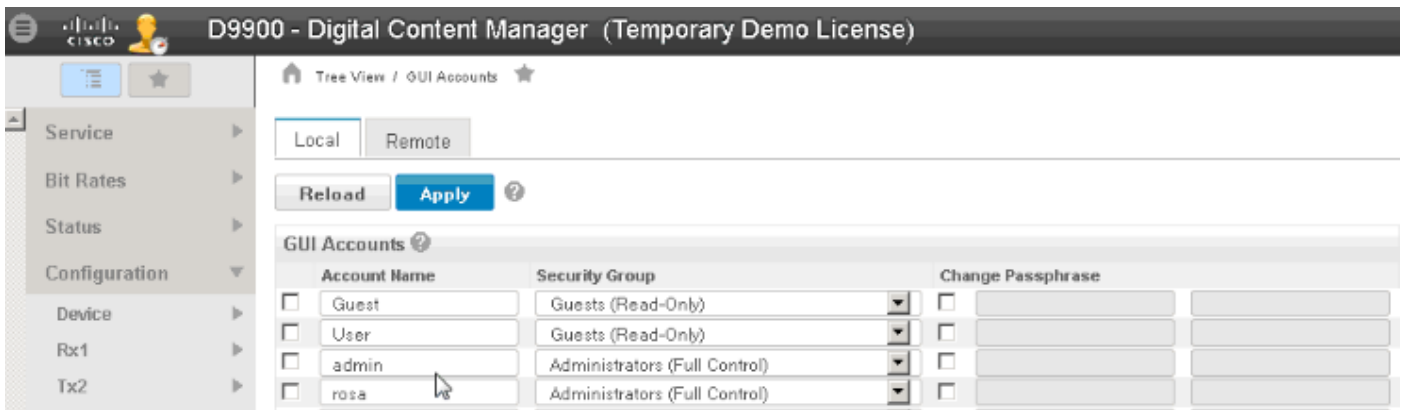
When it has been used for after account creation at the time of the initial configuration, admin account becomes invalid and can no longer be used.

So, that's why you can login with the use of the admin account on 16.10. (admin account was on system and the system has been upgraded with it), but not on newer versions.

Solution

If you are able to log in to the DCM with another login/password, check the GUI Accounts of DCM. Navigate to **Main Menu > Security > GUI Accounts**.

The problem here is if the Account name **admin** (without white spaces) appears.



If it does and you have such an Account name, you need to create a new one for the same Security Group and then delete the Account name admin.

Follow these steps:

1. Log in to the DCM with the use of accounts that belong to the Administrators security group.
2. Select **Security > GUI Accounts** from the main menu. The GUI Accounts page appears.
3. Refer to the **Add new GUI Account** area.
4. In the User Name field, enter a name for the new account (max 40 characters).
5. Select the Administrators (full control) from the drop-down menu of Security Group field.
6. Enter the pass phrase for the new account (maximum 80 characters).
7. Ignore Password Policy field, select **True** to ignore the rules or **False** to apply the configured pass phrase policy rules.
8. Click **Add Account**. The new account is added.
9. Refer to the **GUI Accounts** area.
10. Check the string with admin Account name **admin**.
11. Click the **Remove Checked Items**. The Account name admin will be removed.
12. Click **Apply** at the top of the page.

Note: These GUI account names cannot be used: admin as well as OS account names: root, scriptengine, nobody, sshd.