Troubleshoot CAD and Finesse Desktop Login Issues Related to JTAPI Error

Contents

Introduction
Background Information
Causes and Workarounds
1. Phone's MAC is Not Associated with RMCM Application User on CUCM
2. Extension Mobility (EM) Profile is Not Associated with RMCM User
3. Record Profile with EM
4. Shared Line
5. IPCC Extension Must be on First 4 Lines
6. Allow Control of Device from CTI
7. RMCM Roles
8. Common Device Configuration Profile has IPV6 Enabled
9. RMCM Subsystem Stuck in Initializing

Introduction

This document describes the possible causes and their resolution when desktop login fails because of JAVA Telephony API (JTAPI) issues.

Background Information

The error messages seen when you log into Cisco Agent Desktop (CAD) and Finesse are as shown in these images.

- Error Message on CAD

![Error Message on CAD](image)

- Error message on Finesse

![Error message on Finesse](image)
These are the most common errors that are encountered during the desktop login on CAD/Finesse and there are multiple reasons for this.

**Causes and Workarounds**

1. **Phone's MAC is Not Associated with RMCM Application User on CUCM**

   The MAC address of the phones in which the IP Contact Center (IPCC) extension resides must be selected under Controlled Devices on Resource Manager Contact Manager (RMCM) application user.

   Resolution: Associate the MAC address with the RMCM application user. On the Cisco Unified Communications Manager (CUCM), navigate to User Management > Application User.

   If the MAC of the phone is already associated, then

   1. Disassociate the MAC.
   2. Click **Save**.
   3. Re-associate the MAC.
   4. Click **Save**.

   You can also try to stop and then start the Cisco Computer Telephony Integration (CTI) manager service on all the JTAPI providers.

2. **Extension Mobility (EM) Profile is Not Associated with RMCM User**

   If you use EM together with CUCM 8.0 or later, associate the Device Profile instead of the MAC of the device with the RMCM application user.

   Irrespective of the Device Profile, you associate the application user with, set the **Intra-Cluster multiple Login Behavior Extension Mobility Service** parameter in CUCM to Auto Logout.

   This action helps to overcome the design limitation in CTI/JTAPI noticed in the scenarios, which occur when the **Intra-Cluster Multiple Login Behavior Extension Mobility Service** parameter is set to Multiple Logins Allowed.

   - Agent logs into EM on a phone and also logged in to CAD.
   - If a phone unregisters from CUCM, while the agent is still logged into EM, the phone does not re-register. This failure to register might happen when the agent closes the phone without
logging out of EM or when the network is severed.

- Agent logs into EM from a different device.

- When agents attempt to login to CAD, the system displays the error message "Login failed due to a configuration error with your phone and JTAPI or Unified CM. Contact your administrator".

The bug CSCtx48427 documents this limitation.

3. Record Profile with EM

If CAD agents use Extension Mobility, in which the Device Profile has directory number(s) with Automatic Call Recording option enabled, it can cause login issues, as shown in this image.

This happens because Cisco Unified Contact Center Express (UCCX) is not sent the deviceUnregisteredEvent message, when EM logout happens. This issue happens in CUCM versions prior to 9.X.

The bugs CSCty63105 and CSCty63127 document these limitations.

There is no proper workaround to this issue, but resetting the phone device after logging in to EM has been known to work in some cases. However, this is intermittent.
You can also try to:

1. Disable the **Recording** option
2. Remove the Recording Profile from the Directory Number (DN)
3. Reset the phone

The permanent fix is to upgrade the CUCM to a version that has the bugs already resolved.

### 4. Shared Line

The IPCC extension must not be a shared line.

You can check on the CUCM by navigating **Call Routing > Route Plan Report**. Ensure that the IPCC Extension is unique. There should be no other instance of the DN as seen in this image.

Also, the IPCC Extension must not be part of a Hunt Group.

### 5. IPCC Extension Must be on First 4 Lines

The IPCC extension must be on the first 4 lines on the agent device. UCCX allows more than 4 lines to be configured on the agent device, but monitors only the first four lines, provided these lines are not shared.

### 6. Allow Control of Device from CTI

Ensure that **Allow Control of Device from CTI** check box is checked on the IPCC extension, the phone and on the end user, as shown in this image. If it is already associated, try unchecking and checking it back.
7. RMCM Roles

The RMCM application user must have the group **Standard CTI Enabled** and if you use SIP phone, **Standard CTI Allow Control of Phones supporting Connected Xfer and Conf** as shown in this image.
8. Common Device Configuration Profile has IPV6 Enabled

If the agent phone has **Common Device Configuration Profile** assigned to it, ensure that **IP Addressing Mode** field has **IPV4 Only** assigned to it. In order to check on the CUCM, navigate to **Device > Device Settings > Common Device Configuration** as shown in the image.
9. RMCM Subsystem Stuck in Initializing

When RMCM Subsystem is stuck in Initializing, while opening the CAD application, you get the “Initialization failed, restart the application” error.

If the CAD is already open and you enter the credentials to login, you get the “Login failed due to a configuration error with your phone and JTAPI or Unified CM. Contact your administrator” error.

In order to check, navigate to Cisco Unified CCX Serviceability > Tools > Network Services > Cisco Unified CCX Engine > Subsystem Manager.

RMCM is a subsystem within UCCX that is responsible for monitoring the state of agents and for selecting agents based on the agent’s skills and queue skills required.

Necessary actions to be taken to bring RMCM back in service:

- If RMCM subsystem is stuck in INITIALIZING state on any one node, then
  1. Disable CDS/HDS
  2. Reset Replication
  3. Enable CDS/HDS.

- Reset the RMCM user password on UCCX, save it and restart the UCCX engine. If it’s a HA, Restart the engine on both nodes.

- Create a new RMCM provider user. Creating the user on UCCX propagates it to the CUCM.
In UCCX version 9.0.1, 9.0.2.10000-71 (9.0.2 base) and 9.0.2.11001-24 (9.0.2 SU1) RMCM is stuck in initializing state if the JMX logs are full. Check if the disk login is full by running the show status command on the CLI of the affected server.

```
admin:show status
```

```
Host Name    : pub9
Date        : Wed May 13, 2015 07:14:53
Time Zone   : India Standard Time (Asia/Kolkata)
Locale      : en_US.UTF-8
Product Ver : 9.0.2.11001-24
OS Ver      : 5.0.0.0-2
License MAC : 0183a27e0bc7

Uptime:
07:14:54 up 3 days, 21:35, 1 user, load average: 0.74, 0.81, 0.67

CPU Idle:   88.12%  System: 00.00%  User: 09.90%
IOWAIT:    01.98%   IRQ: 00.00%   Soft: 00.00%   Intr/sec: 263.37

Memory Total: 6097316K
  Free: 2412372K
  Used: 3684944K
  Cached: 1990132K
  Shared: 0K
  Buffers: 297104K

<table>
<thead>
<tr>
<th>Disk Type</th>
<th>Total</th>
<th>Free</th>
<th>Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk/active</td>
<td>26657340K</td>
<td>15888436K</td>
<td>10493712K (40%)</td>
</tr>
<tr>
<td>Disk/inactive</td>
<td>27087452K</td>
<td>18957564K</td>
<td>7854696K (30%)</td>
</tr>
<tr>
<td>Disk/logging</td>
<td>92738892K</td>
<td>40350056K</td>
<td>47601872K (100%)</td>
</tr>
</tbody>
</table>

The bugs CSCul18667 and CSCun54915 document this behavior.

After the JMX logs are deleted as per the defect CSCul18667, you need to contact the Technical Assistance Center (TAC) to perform the workaround of the defect CSCun54915 mandatorily. If workaround of CSCun54915 is not performed then after the server reboot, UCCX engine does not come up.

- If you are on CCX 8.5 SU1 or below, RMCM can be stuck in initializing state when no agents are created as depicted by the bug CSCtq84602.

You can always restart the CTI-Manager on all the CUCM nodes. Deleting the Identity Trust List (ITL)/Certificate Trust List (CTL) files of the phone helps.

If the above workarounds are not useful, open a TAC case.