Troubleshoot CPS Control Center Session Limit Issue

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Background Information](#)
[Problem](#)
[Procedure to Resolve CPS Control Center Session Limit Issues](#)
[Approach to Clear Max Session Limit per User Exceed Alert](#)
[Approach to Customize Session Limit per User](#)

Introduction

This document describes the procedure to troubleshoot Cisco Policy Suit (CPS) Control Center Session Limit issues.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Linux
- CPS

Note: Cisco recommends that you must have privilege root access to CPS CLI.

Components Used

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

- CPS 19.4 and earlier versions.
- Unified Computing System (UCS)-B

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.

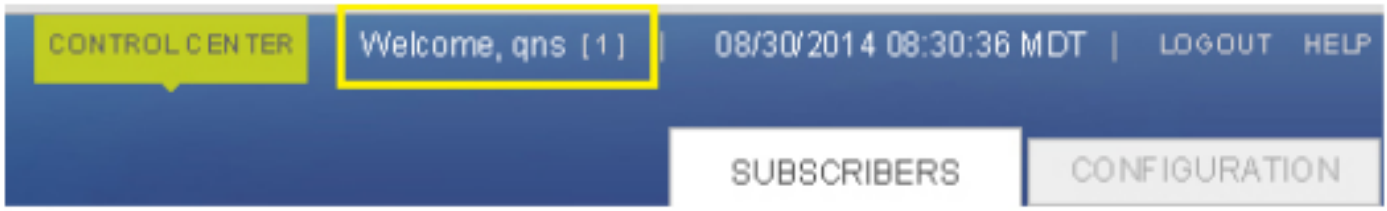
Background Information

CPS Control Center GUI enables you to do these tasks:

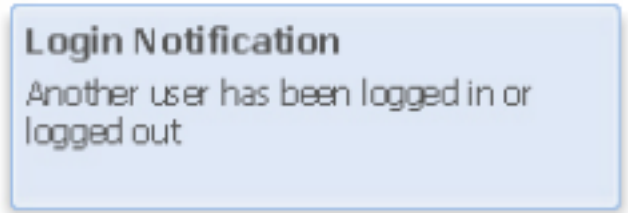
• Manage subscriber data, that is, find or create and edit information about your subscribers.
• View subscriber sessions.
• View system sessions.
• Populate custom reference data (CRD) tables.

CPS Control Center supports session limits per user. If the user exceeds the configured session limit, they are
not allowed to log in. CPS also provides notifications to the user when other users are already logged in.

When a user logs in to Control Center, a Welcome message displays at the top of the screen. A session counter is shown next to the username. This represents the number of login sessions for this user. In this example, this user is logged in only once ([1]).



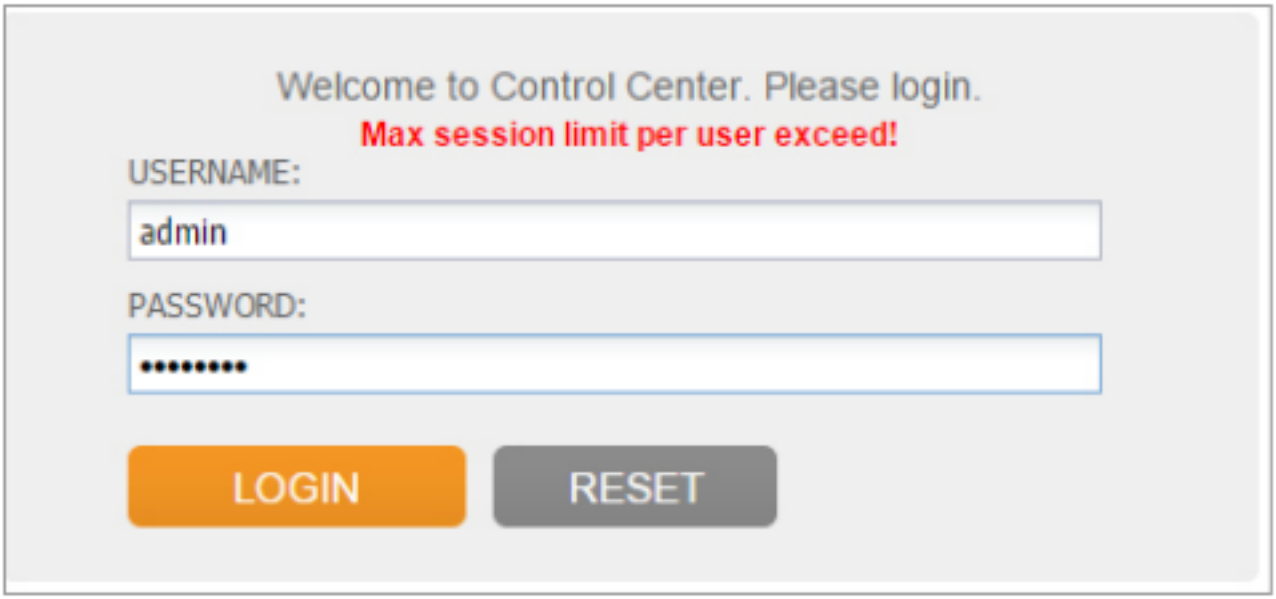
Welcome Message



Login Notification for a Second User

Problem

When the number of sessions the user exceeds the session limit, the user is not allowed to log in and receives the message **Max session limit per user exceed!** as shown in the image.



Error

Message on "Max session limit per user exceeded"

The session limit can be configured by the runtime argument, which can be configured in the qns.conf file. **-Dcc.user.session.limit=XX** (default value is 5).

Procedure to Resolve CPS Control Center Session Limit Issues

Approach to Clear Max Session Limit per User Exceed Alert

Step 1. Run this command from the installer to login into the OSGi framework of CPS.

```
[root@installer ~]# telnet qns01 9091
Trying 192.168.10.141...
Connected to qns01.
Escape character is '^]'.

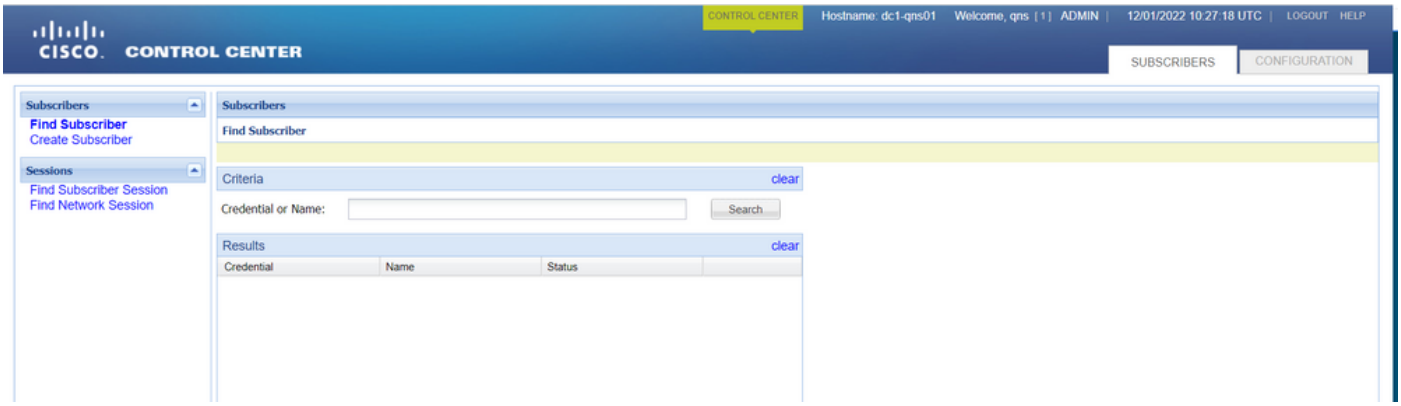
osgi>
```

Step 2. Run this command to flush all control center user sessions.

```
osgi> flushCCSessions
Successfully flushed all control center user session.

osgi>
```

Step 3. Try to login into Control Center as a fresh browser session and verify that you are able to log in with the desired username. If you are able to log in to Control Center GUI, then you can ignore the rest of the steps in this approach.



Control CenControl Center GUI home pageter GUI home page

Else if you are still unable to log in to Control Center due to the **Max session limit per user exceed!** alert, then proceed with Step 4. onwards.

Step 4. Run this command from the Installer to log in to the active LB of the impacted CPS.

```
#ssh lbvip01
```

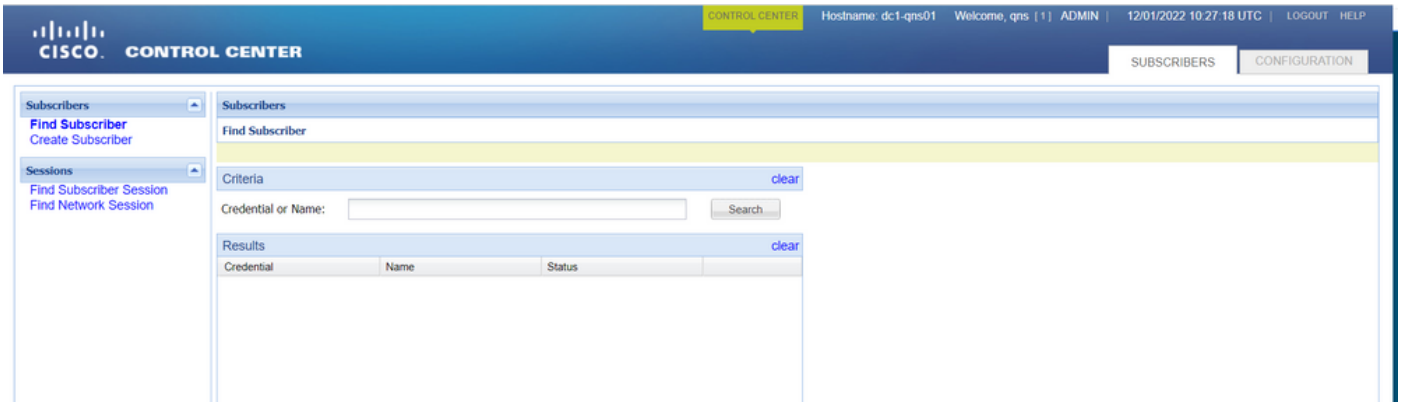
Step 5. Run this command to restart the **Memcached** process in active LB to clear the **Max session limit per user exceed!** alert in Control Center GUI.

```
#monit restart memcached
```

Alternatively, these commands can also be used to restart the **Memcached** process.

```
#service memcached stop
#service memcached start
```

Step 6. Try to login into Control Center as a fresh browser session and verify that you are able to log in with the desired username.



Control CenControl Center GUI home pageter GUI home page

Approach to Customize Session Limit per User

Note: This approach is applicable for recent CPS versions as well.

Step 1. Login into Cluster Manager as a **root** user.

Step 2. Backup qns conf file.

```
[root@CM ~]$ cp /etc/broadhop/qns.conf /etc/broadhop/qns.conf.$(date +%m%d%Y).bkp
```

Step 3. Add **-Dcc.user.session.limit=15** to **/etc/broadhop/qns.conf.**

```
[root@CM ~]$ sed -i '$ i -Dcc.user.session.limit=15' /etc/broadhop/qns.conf
```

Note: Session limit count 15 is provided as a sample only.

Step 4. Build puppet script.

```
[root@CM ~]$ /var/qps/install/current/scripts/build/build_etc.sh
```

Step 5. Distribute the modified file to all VMs.

```
[root@CM ~]$ copytoall.sh /etc/broadhop/qns.conf
```

Step 6. Validate qns conf is updated in other VMs.

```
[root@CM ~]$ ssh pcrfclient01
[root@cc ~]$ grep 'Dcc.user.session.limit' /etc/broadhop/qns.conf
Expected output: -Dcc.user.session.limit=15
```

Step 7. Restart all QNS services. Run this command from Cluster Manager.

```
[root@CM ~]$ /var/qps/bin/control/restartall.sh
```