

TECHNICAL SUPPORT BULLETIN

March 4, 2020

TSB 2020-004 – IoT 1.5 Upgrade and Insufficient Licenses

SEVERITY: Medium

PRODUCTS AFFECTED: RUCKUS IOT

BULLETIN OVERVIEW

This bulletin describes a condition that may affect your IoT network after upgrading the Ruckus IOT controller to 1.5 and installing licenses on the controller.

PROBLEM STATEMENT

Performing a firmware upgrade Ruckus IOT controller from earlier version than IOT 1.5 or upon installing a fresh instance of IOT 1.5, we require IOT controller to have licenses installed for [RTU Instance](#) and [AP capacity](#). The AP capacity licenses are used to manage the IOT AP's by the controller. However, these licenses are assigned to the AP on first come first served basis and the controller does not currently look for the IOT modules connected to the AP's.

RISK ASSESSMENT

If the IOT controller does not have enough AP capacity licenses to support all AP's in the network, then this may lead to a situation where some of the AP's, containing an AP module, may stay in an unregistered state.

SYMPTOMS

After installing/upgrading to IOT 1.5 Release, APs can stay in unregistered state.

ROOT CAUSE

AP capacity licenses on IOT controller are applied to AP's on first come first served basis and it is not dependent on whether APs have an IOT module installed.

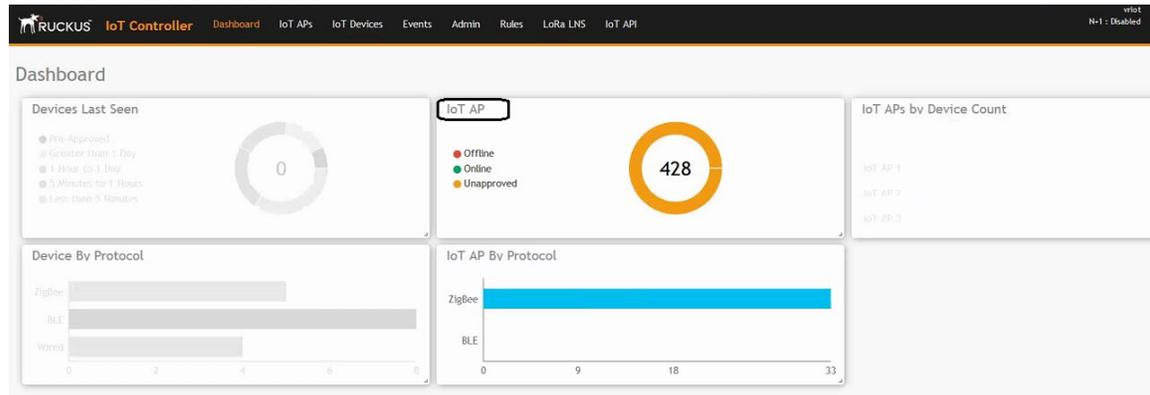
TROUBLESHOOTING

Ensure that the IOT controller is up and running and it have enough AP capacity Licenses installed i.e Total AP Capacity License \geq Total IOT AP's.

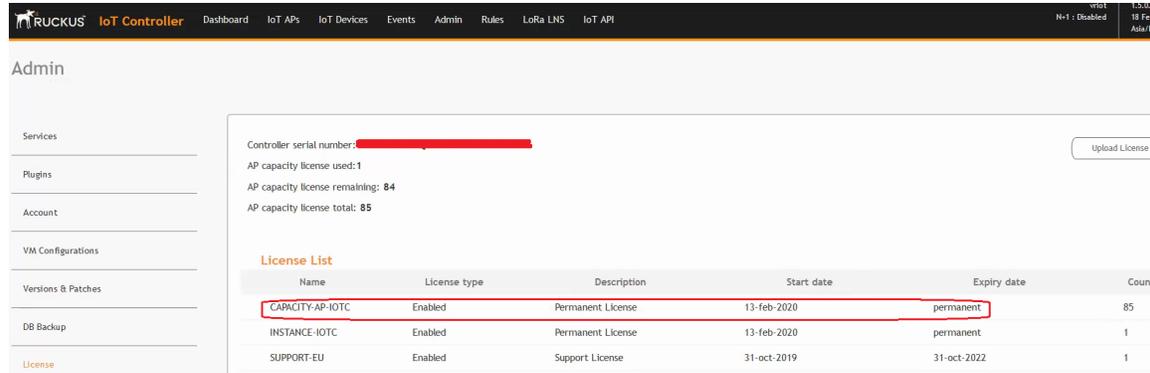
In case Total AP Capacity licenses are less that the Total AP's, we might need to delete the AP's from IOT controller which do not have an IOT module installed.

Example:

Total AP's on IOT controller



Total IOT AP licenses:



According to above scenario, only 85 AP's can be managed by the IOT Controller.

WORK AROUND

The work around is -

1. Remove all AP's from the IOT controller.
2. Set IoT enable on the APs with installed IoT module.
3. Add IoT Controller IP address manually on the APs with an IoT module.

Step#1: First of all, we need to remove all AP's from the IOT controller by disabling IOT and pointing them all to a dummy IP using following AP CLI script:

```
#define AP FW version
fw_version=<define the firmware version of SZ>
#define Model class
model=all
# Command
set iotg-enable 0
set iotg-mqtt-brokerip 1.1.1.1
```

Save above script in text format and apply to SZ from Diagnostics>Scripts> AP CLI Script.

Step#2: Once All AP's have IOT disabled, we need to delete all AP's from the IOT controller. We can either do a bulk delete by selecting all AP's or we can reset the IOT controller to factory default and that will remove all IOT AP's.

Step#3: Next step is to connect desired AP's with IOT module installed to the IOT Controller. There are few ways to do that depending on the network size:

If there are only a few AP's with an IOT module, setting the IOT IP manually via the AP CLI would be the quickest way:

```
set iotg-enable 1
set iotg-mqtt-brokerip <IP of vRIOT controller in x.x.x.x format>
```

Isolate IoT APs and non-IoT APs at Layer 2 (VLAN) or Layer3 (IP) subnets. In this case, DHCP Option 43 Sub-Option 21 can be configured for networks with APs meant to be connected with a particular IoT Controller. This is done by the network administrator.

Move desired AP's with an IOT module installed to a different(New) Zone on the SZ and run AP CLI script to push ONLY those APs to IOT controller. Below is a sample script to set the IOT controller's IP and enable IOT state on the AP:

```
#define AP FW version
fw_version=<define the firmware version of SZ>
#define Model class
model=all
```

Command

```
set iotg-enable 1
```

```
set iotg-mqtt-brokerip <IP of vRIOT controller in x.x.x.x format>
```

Once this script is applied, ONLY AP's from the newly created Zone will move to IOT controller.

CORRECTIVE ACTION

TBD