Restrict connections by SSID

- As more and more people start to deploy RADIUSdesk there are always new places and ways RADIUSdesk are being deployed.
- One such a deployment required that:
    - There be some restrictions imposed based on the SSID which the user connected to.
    - A user will be allowed to connect to one or more SSIDs.
    - This restriction will not depend or require that the packet comes from a certain vendor's equipment.
    - We have an easy way to manage the list of SSIDs.
- With the list of requirements, a quick fix was out of the question.

How does a quick-fix look

- We assume the incoming packet comes from a Ruckus Zonedirector.
- The incoming packet will then contain a Ruckus specific AVP for SSID:

```
Ruckus-SSID = "Test2"
```

- We can then simply add a private check attribute per user: That **Ruckus-SSID**(AVP) **==** (Operator) **Test2**(Value).
- This unfortunately limits us to one value, one vendor and we have no easy way to get a list of all the SSIDs.

Since the quick fix did not fulfill all our desires we invented something which does: **The SSIDs applet**

The SSID applet

- The SSID applet lives under **Menu→Realms and Providers→SSIDs**.
- This is the place where you **C**reate **R**ead **U**pdate and **D**elete (**CRUD**) the pool of SSIDs.
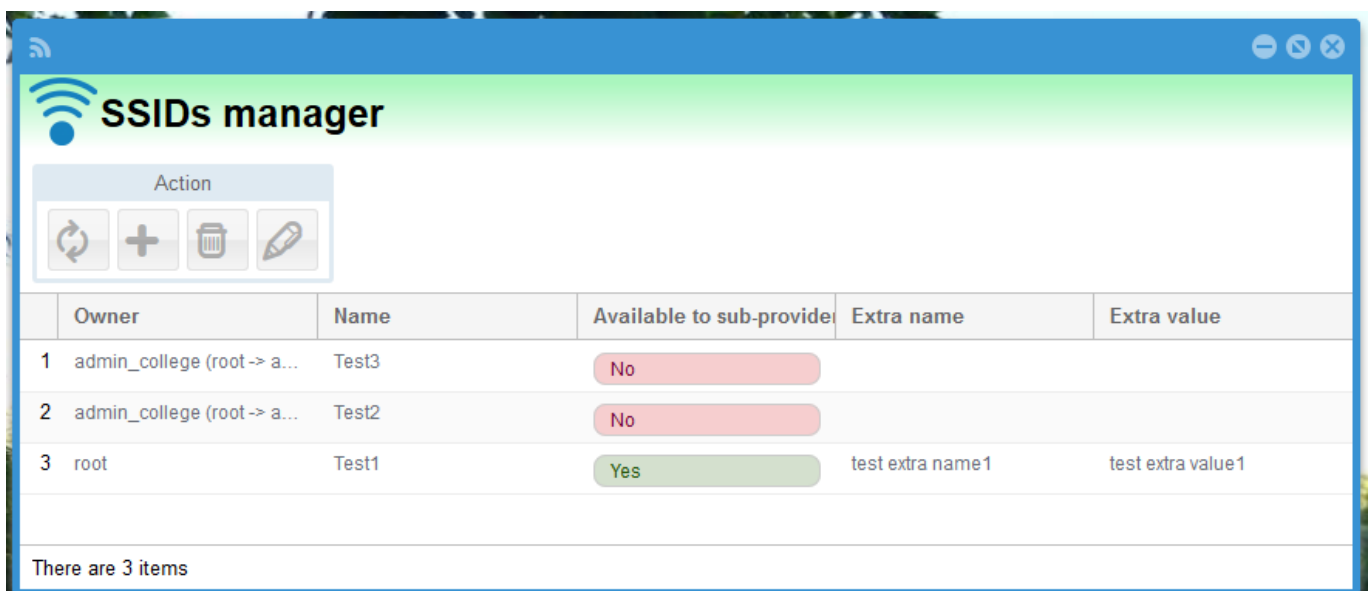
- Once we have our pool of SSIDs we can attach one or more to either a **Voucher** or **Permanent user**.

- This feature is a **NON disruptive** feature. This means that there are no harm done if you **do not** use it.

How do we do it?

- This section is for the technical minded who like to know how things work.
- We added two internal AVPs:
    - Rd-Ssid-Check
    - Rd-Ssid-Value
- We also added a **user_ssids** table to the SQL database where the username and SSIDs which the specific username are allowed to connect from is kept.
- This mapping is managed through the RADIUSdesk front-end.
- **Rd-Ssid-Check** is added to a Permanent User or Voucher's name in the **radcheck** table with a value of **1** to enforse SSID restrictions.
- We use the **Rd-Ssid-Value** internal AVP to store the value of the SSID which we filter out of the incoming RADIUS Auth packet's **Called-Station-Id**.

- This will typically be in the format of [MAC address]:[SSID].
- Below is the logic we added to the policy.conf file.
- Here we grab the SSID if available

```
RADIUSdesk_rewrite_called_station_id {
    if(Called-Station-Id =~ /^([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:.]?([0-9a-
f]{2})[-:]?([0-9a-f]{2})[-:.]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([-a-
z0-9_. ]*)?/i){
        if("%{7}"){
            update control {
                Rd-Ssid-Value := "%{7}"
            }
            updated
        }
    else {
            noop
        }
    }
    else {
        noop
    }
}
```

- Here we check if we need to enforce this SSID check

```
RADIUSdesk_user_ssid_check {
    #__We check if the user is flagged to only connect through certain SSIDs
(Rd-Ssid-Check == 1)_
    #__If so we try to find the SSID and see if this ssid is allowed for the
specific user_____

    #If it is present....
    if("%{control:Rd-Ssid-Check}"){
        #If it is == 1
        if("%{control:Rd-Ssid-Check}" == 1){
            RADIUSdesk_rewrite_called_station_id
            if(updated){
                if("%{sql:SELECT COUNT(*) FROM user_ssids WHERE username=
'%{request:User-Name}' AND ssidname= '%{control:Rd-Ssid-Value}'}" > 0){
                    ok
                }
                else {
                    update reply {
                        Reply-Message := "User %{request:User-Name} has not
permission to connect through SSID: %{control:Rd-Ssid-Value}"
                    }
                    reject
                }
            }
            else {
                update reply{
```

```
            Reply-Message := "No SSID available to evaluate SSID
restriction"
                }
                reject
            }
        }
    }
}
```

From:
https://radiusdesk.com/docuwiki/ - **RADIUSdesk**

Permanent link:
https://radiusdesk.com/docuwiki/user_guide/restrict_by_ssid

Last update: **2016/06/02 23:08**