Virtual SmartZone

Setup Guides and Tutorials for the Ruckus Virtual SmartZone

- Creating DHCP Server/VLAN on vSZ APs
- How to Configure and Optimise SmartRoam on vSZ
- Advanced Guide: LDAP Authentication on Ruckus vSZ via Azure AD Domain Services (Azure AD DS)
- How to Configure and Optimise SmartRoam on vSZ

Creating DHCP Server/VLAN on vSZ APs

Introduction

DHCP/NAT functionality on SZ-managed APs and DPs (data planes) allows customers to reduce costs and complexity by removing the need for DHCP server/NAT router to provide IP addresses to clients.

Three general DHCP scenarios are supported:

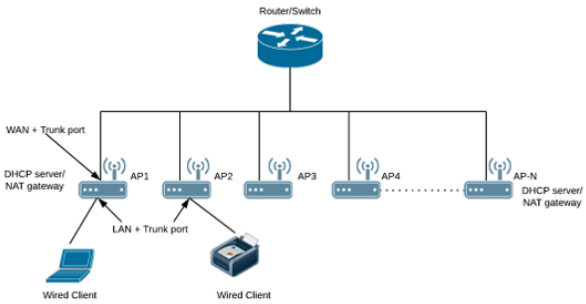
- SMB Single AP: DHCP is running on a single AP only. This AP also functions as the Gateway AP.
- SMB Multiple APs (<12): DHCP service is running on all APs, among which two of the APs will be Gateway APs. These two Gateway APs will provide the IP addresses as well as Internet connectivity to the clients via NAT.
- Enterprise (>12): For Enterprise sites, an additional on-site vSZ-D will be deployed at the remote site which will assume the responsibilities of performing DHCP/NAT functions. Therefore, DHCP/NAT service will not be running on any APs (they will serve clients only), while the DHCP/NAT services are provided by the onsite vSZ-D.

Single AP Topology

All the APs in the zone get their IP from the WAN router and provides the DHCP/NAT service. If H510/H320 is configured as GAP by the manual port selection, then LAN1 and LAN2 configuration will be pushed to eth1 and eth2 ports of H510/H320 APs instead of eth0 and eth1 ports.

Each AP in this zone is running it’s own DHCP server instance.
Typically configured when APs are at different sites and roaming is not required.

Figure 1. Single AP Topology

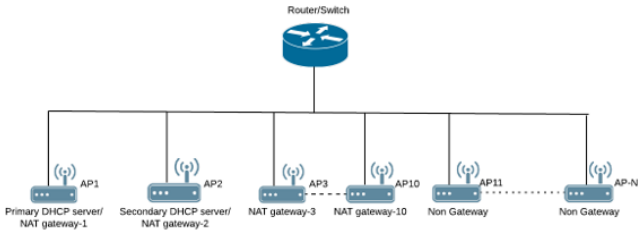


Multiple AP (Flat Network) Topology

All the APs in the zone get their IP from the WAN router and designated APs to provide the DHCP/NAT service. A maximum of two APs be can select for DHCP service (Primary and Secondary) and ten APs for NAT Gateway.

Designated APs in this zone are running the DHCP Server instance.
Typically configured when multiple APs are at the same site and roaming across APs is needed.

Figure 2. Multiple AP (Flat Network) Topology

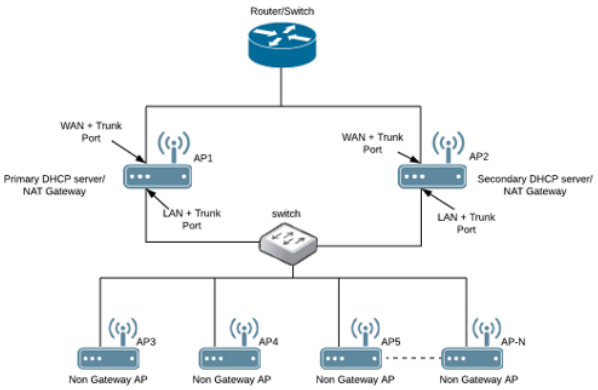


Hierarchical AP Topology

Designated APs provide the DHCP/NAT service. Gateway APs (GAPs) get the IP address from the WAN router and non-gateway APs get the IP from the Gateway APs. If H510/H320 is configured as GAP by the manual port selection, then LAN1 and LAN2 configuration will be pushed to eth1 and eth2 ports of H510/H320 APs instead of eth0 and eth1 ports. In order to configure eth0 ports of H510/H320, the user needs to configure LAN5/LAN3 Ports respectively for the H510/H320 APs.

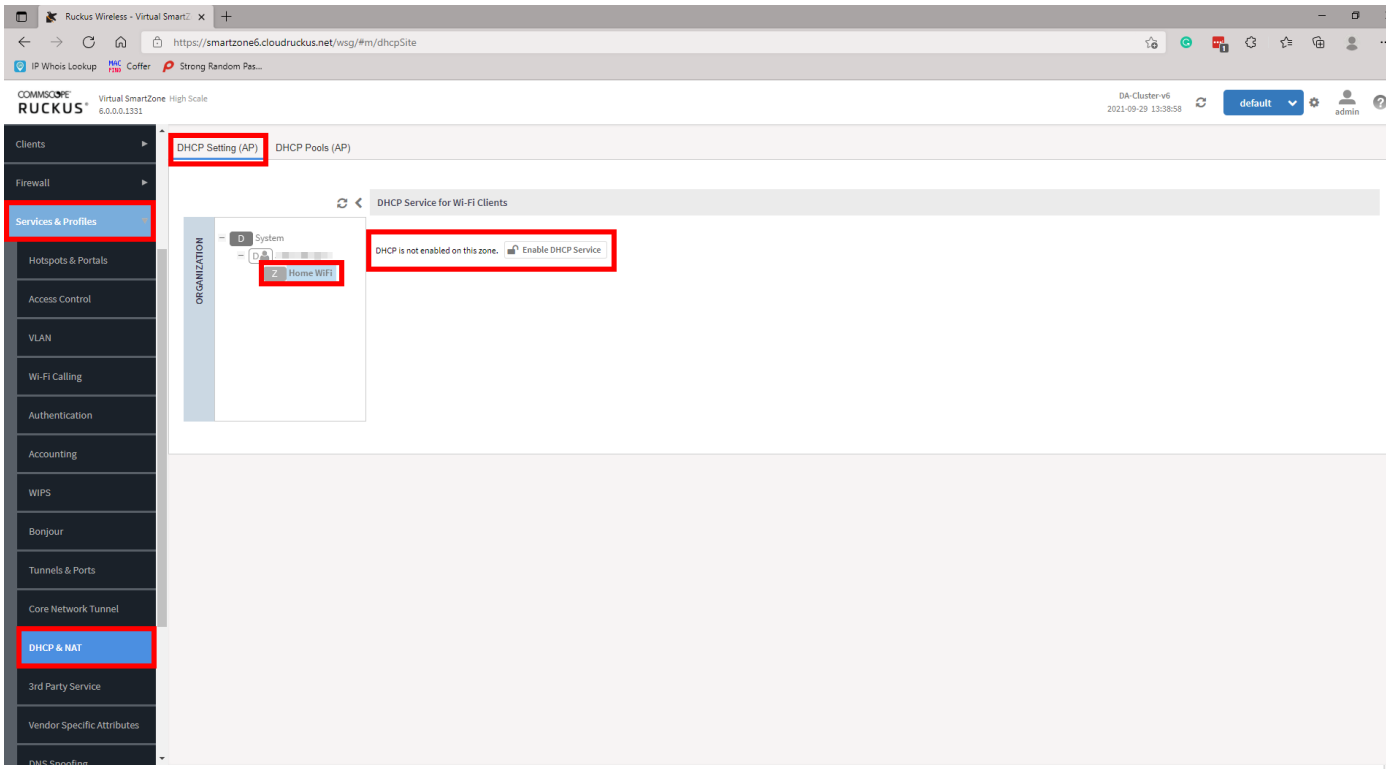
Designated APs in this zone are running the DHCP Server instance.
The DHCP server APs connected to the WAN, the rest of APs get their Private IP address from a local IP Pool with VLAN ID 1 from the DHCP Server AP.

Figure 3. Hierarchical AP Topology

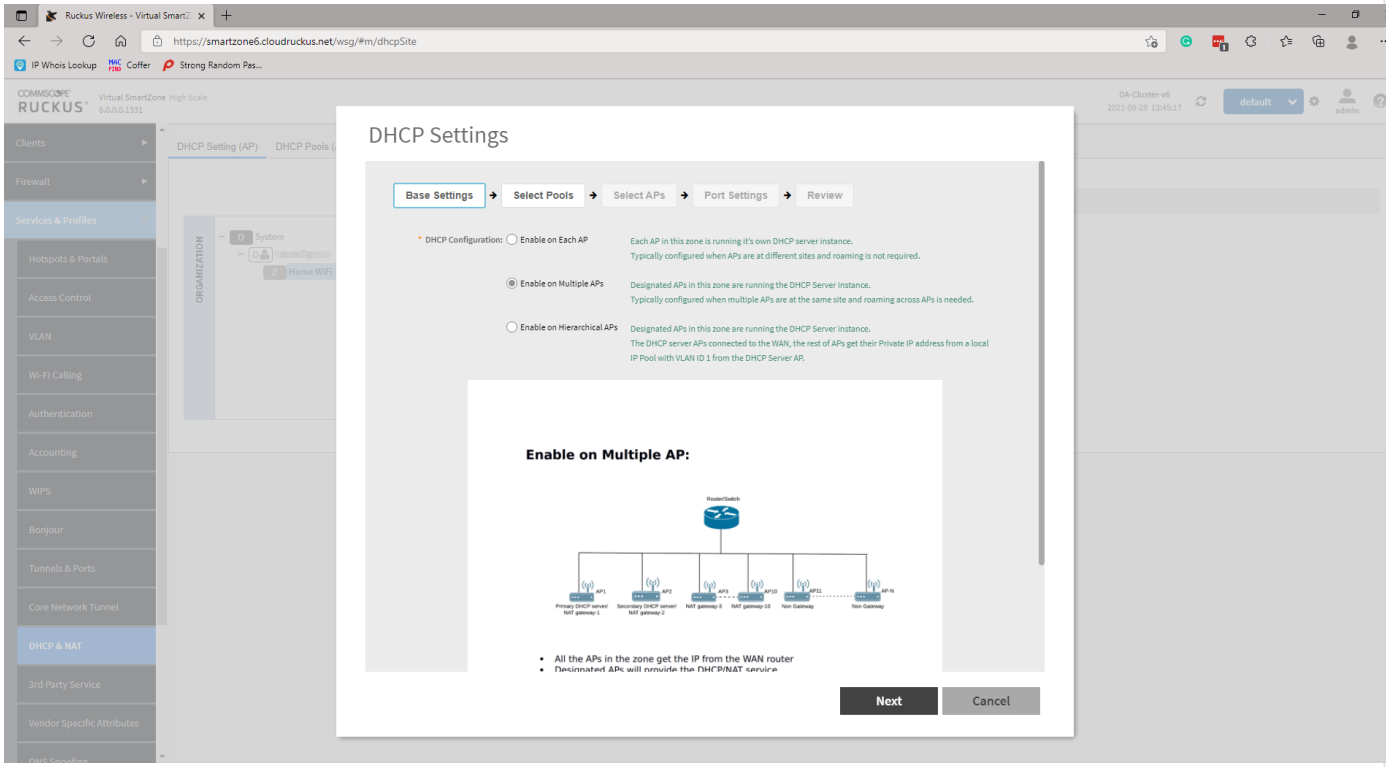


Method

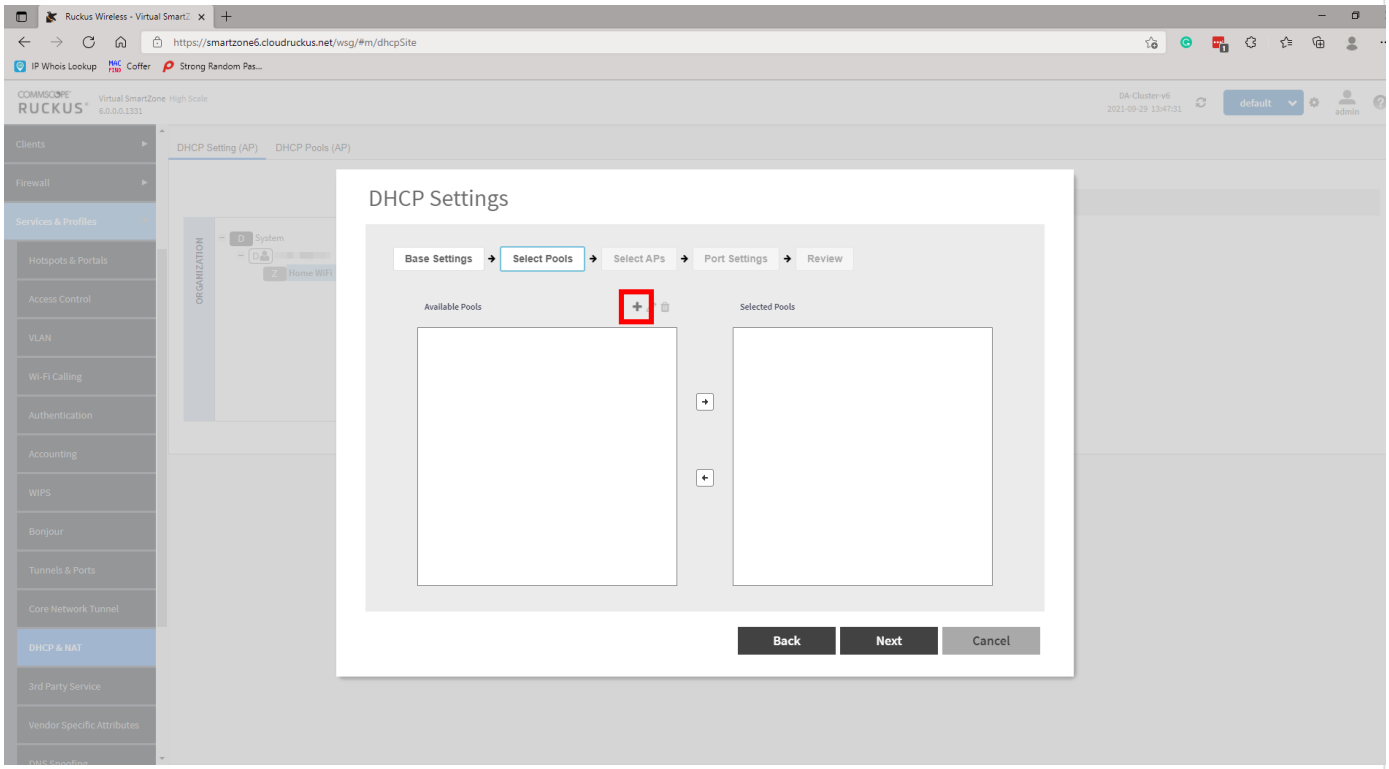
Login to the vSZ and Navigate to **Services and Profiles** then **DHCP & NAT**. Locate the domain under the organisation pane, then expand the required domain and highlight the zone you wish to configure your DHCP service. There will be an option to **Enable DHCP Service**. Enable this, to be directed through a configuration wizard.

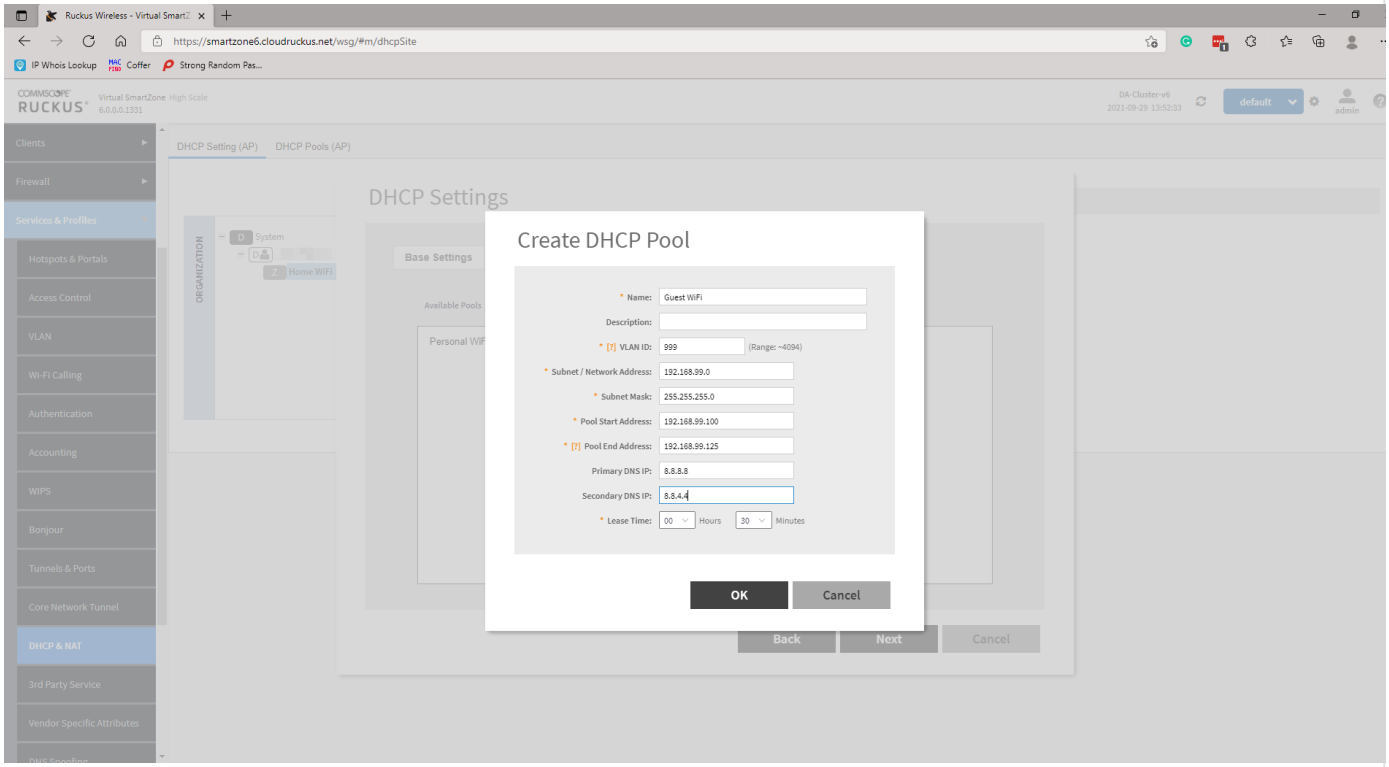


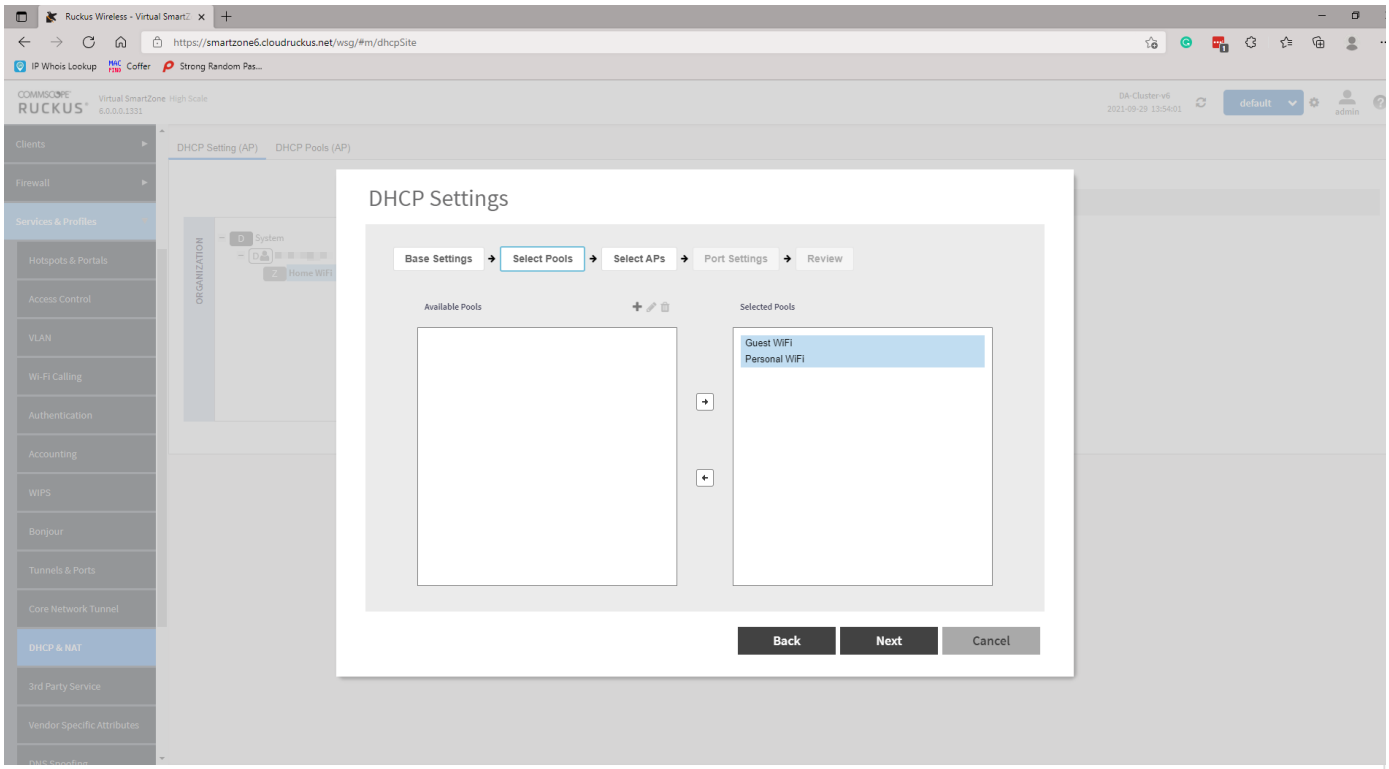
Select the appropriate **Base Settings**. The options are **Single AP** (1), **Multiple APs** (<12), or **Hierarchal APs** (>12). For the purpose of this KB we will only be looking at **Single AP** or **Multiple AP** scenarios as Hierarchal will require a data plane. Click **Next** to continue.



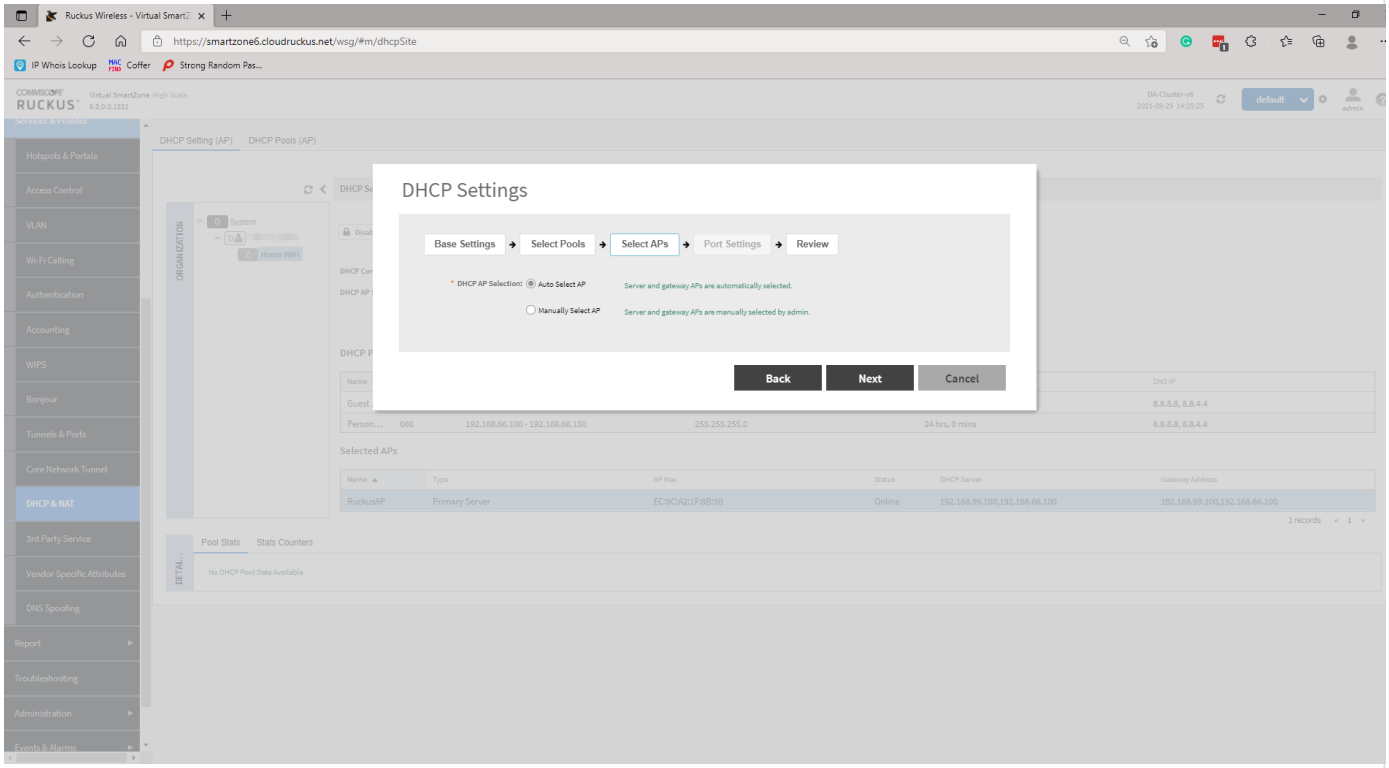
Create a **DHCP Pool** by clicking on the **+**. A new page will pop up. Simply enter the required information and click **OK**. Repeat more networks if necessary. Once done, highlight and move the Pools from **Available Pools** to **Selected Pools** and click **Next** to continue.

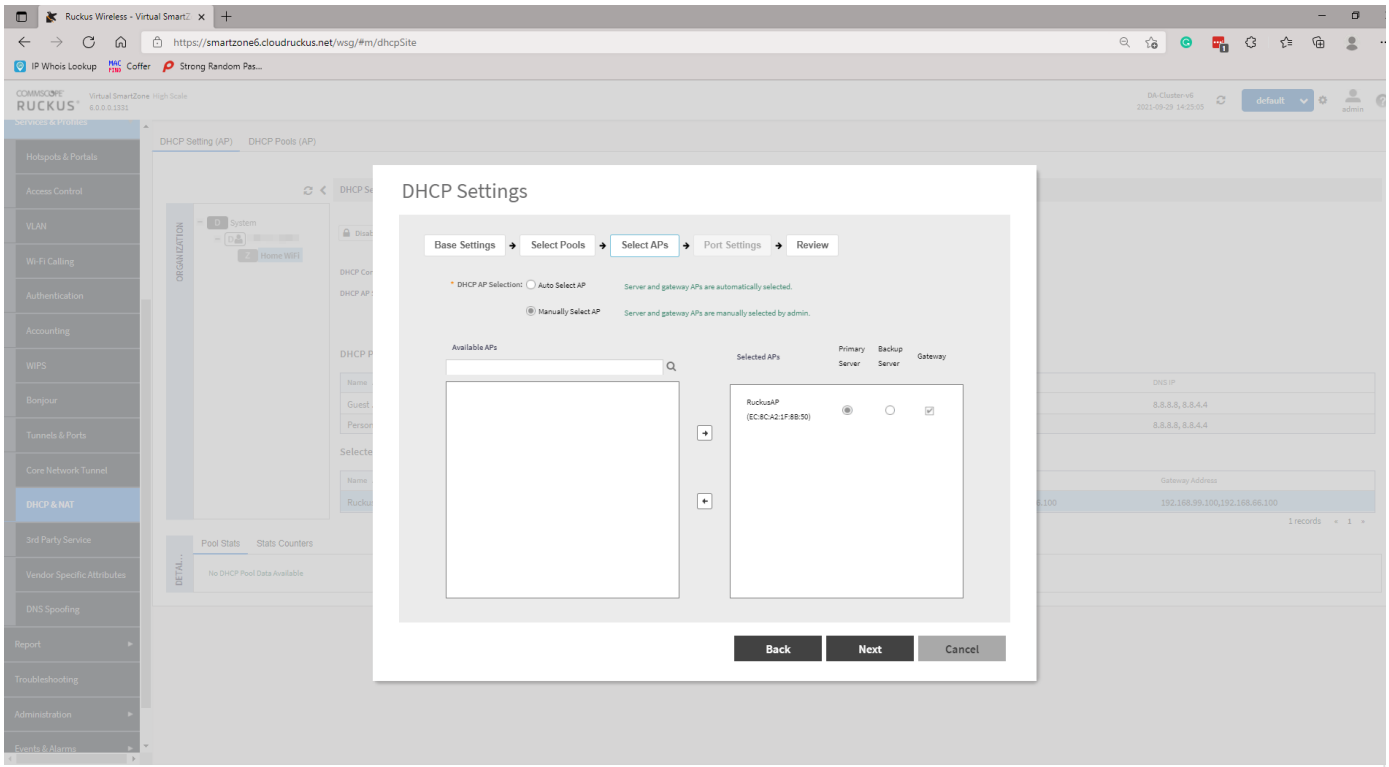




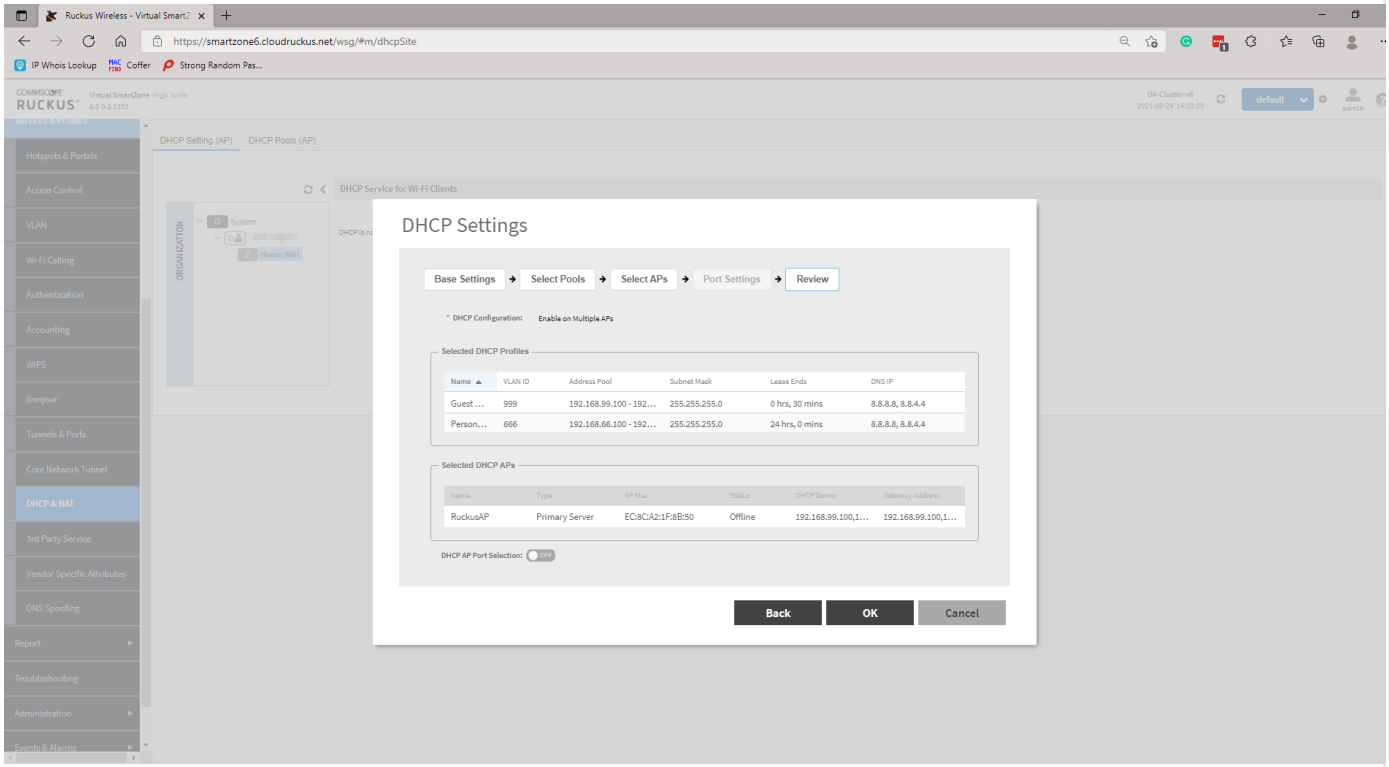


On the next page, select your **Gateway AP(s).** The options are either **Automatic** or **Manual**. If you are selecting **Manual**, you will need to move AP(s) similar to moving the Pool(s) in the previous step and select a Primary and Secondary AP. Click **Next** to continue.

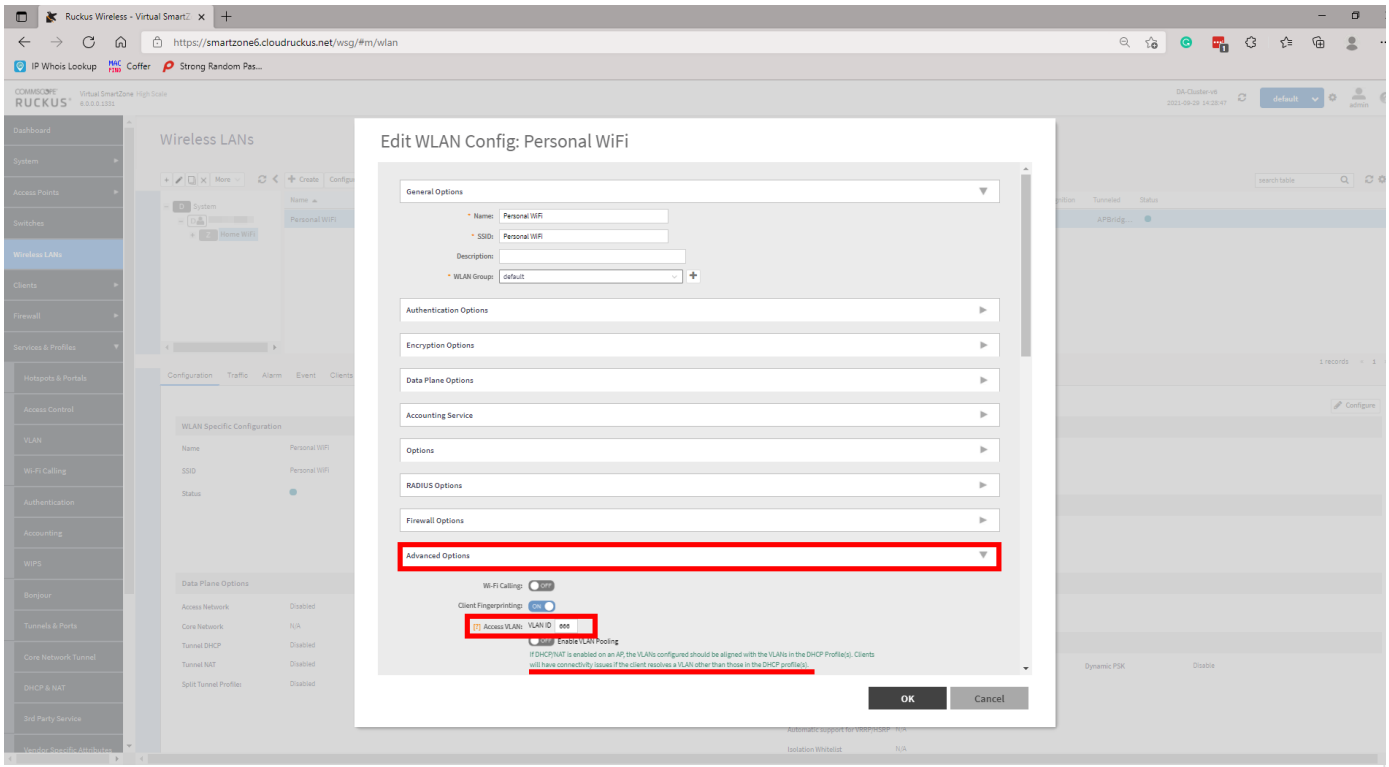




Review your configuration and click **OK** to confirm.



Configure your WLANs now as you normally would, however, ensure that under **Advanced Options** that your **Access VLAN** is set as per your DHCP profile.



Perform testing to ensure all is working as expected.

To prevent the two network users from being able to communicate with one another you must now create **L3 Access Control** profile(s). This will look something like the following:

Action: Block

Source Network Address/Subnet Mask

Destination Network Address/Subnet Mask

So for example, if we want to block communication between our Private and Guest wireless networks we will need to create two rules and affix these to the respective WLAN.

Block Guest on Private

Action: Block

Source 192.168.66.0/24

Destination 192.168.99.0/24

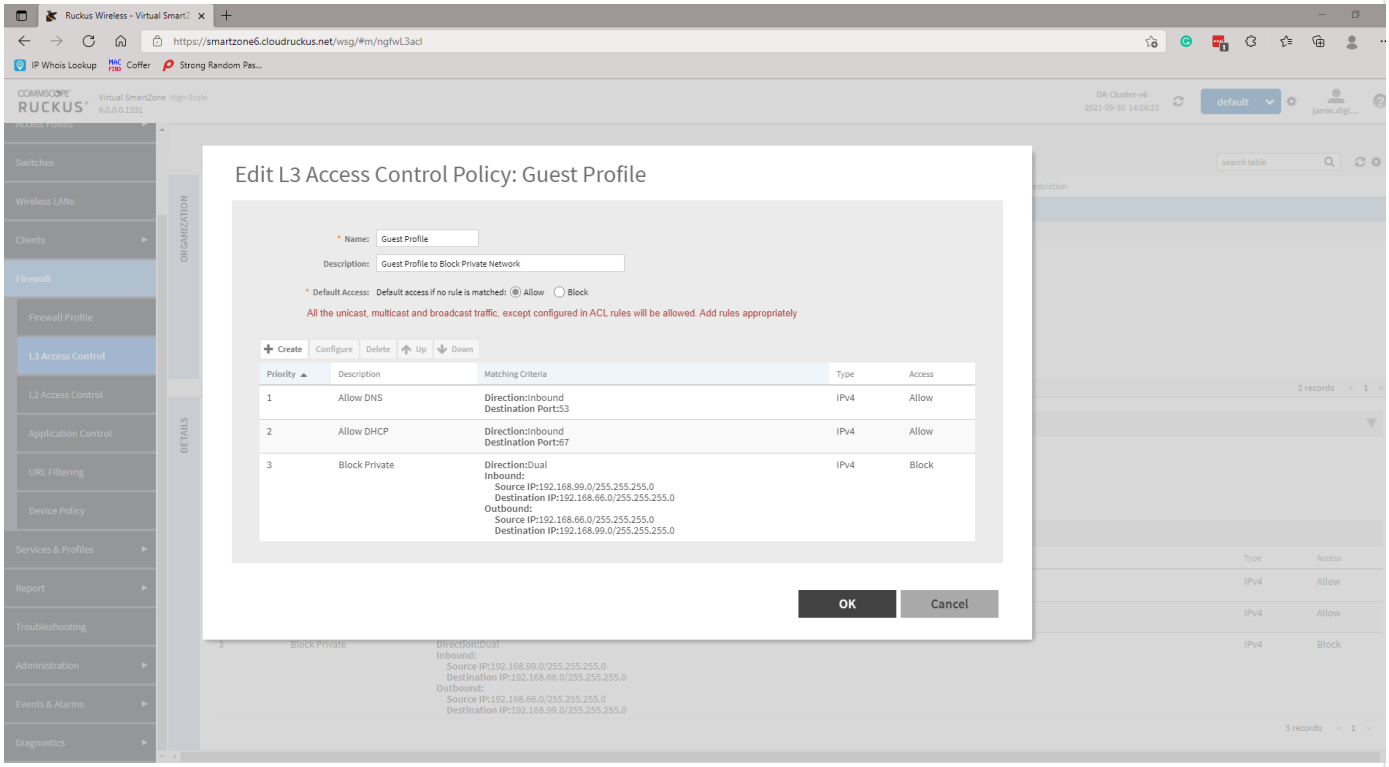
Block Private on Guest

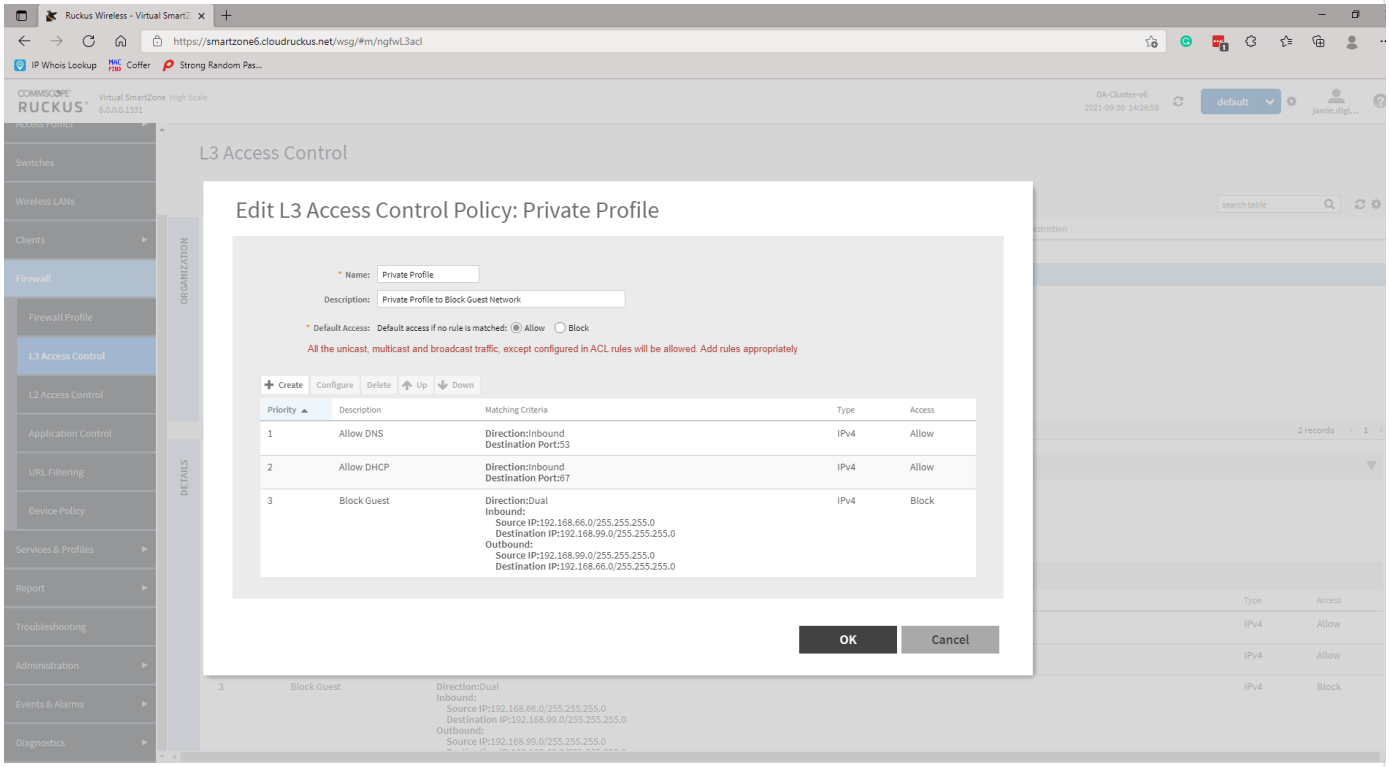
Action: Block

Source 192.168.99.0/24

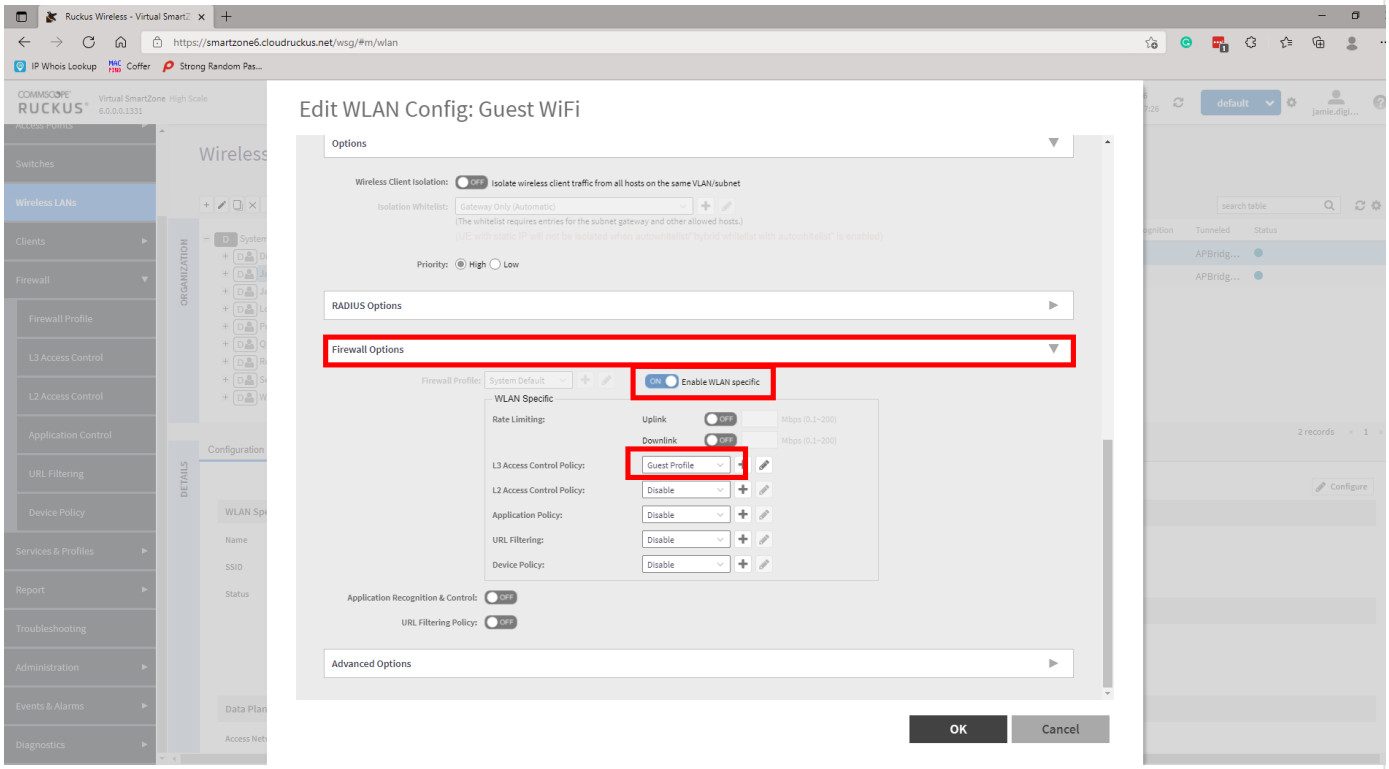
Destination 192.168.66.0/24

Navigate to **Firewall** then **L3 Access Control**, highlight the appropriate domain then click **Create**. A new page will pop up. Provide a **Name** and **Description** and create a rule by clicking **Create**. Add a **Description**, under **Access** select **Block** from the drop-down. Enter the **Source** and **Destination Network Address** and **Subnet Mask**. Set the **Direction** to **Dual**. Create profiles for any necessary networks.





Apply these to your WLANs by navigating to **Wireless LANs**, highlight and configure your WLAN, scroll down to **Firewall** and select the tickbox for **Enable WLAN specific**. Under the **L3 Access Control Policy** use the dropdown to select the appropriate profile. Repeat for all necessary WLANs.



Perform testing to ensure all is working as expected.

Notes

- There is a limitation of 1000 IPs per DHCP Pool
- When running SMB **Multiple AP** mode, 10 IPs will be reserved for Gateway APs
- You can navigate to **Services and Profiles** then **DHCP & NAT** to obtain information on the DHCP server stats

How to Configure and Optimise SmartRoam on vSZ

Introduction

Some clients do not roam even if they are physically moved to a new location. Not all clients have roaming aggressiveness setting to fine-tune roaming. Apple devices are reported to cling to the AP they first learn an SSID on.

In a multi-AP environment, a client will always be looking for the best AP to connect to. It will remain connected to its current AP and roam to an adjacent AP once the signal level falls below a certain threshold. This behavior ensures best possible performance at all times.

To achieve this, a client must be doing background scanning to learn about its environment. Frequency of this background scan can determine the roaming behavior. Certain clients such as Windows clients allow roaming aggressiveness to be tweaked. "High" setting will make the client to perform background scanning more often to learn about available APs to connect. While the "Low" setting will make the client do less frequent scanning. This setting can be found under the wireless adapter properties.

Unfortunately, this tweaking is not readily available for all client types. For example, various smartphones and Apple clients do not provide this setting to encourage roaming.

For these types of clients, it is obvious to look towards infrastructure for help. Ruckus has added firmware support to disconnect a client if its signal falls below the user-definable threshold. This feature is called SmartRoam. With this feature, there will be an explicit disassociate message to kick off the client.

Method

This is a per-SSID setting as illustrated above. "smart-roam" parameter takes values from 1 to 10.
These are called roam factors, and they map to an RSSI value in dB as per the list below:

Mapping of roaming factor, to RSSI.

RSSI threshold (dB) 'roam_rssi_thrlo'	Scale Factor (#) 'roam_factor'
5	1
10	2
15	3
17	4
20	5
23	6
27	7
32	8
40	9
60	10

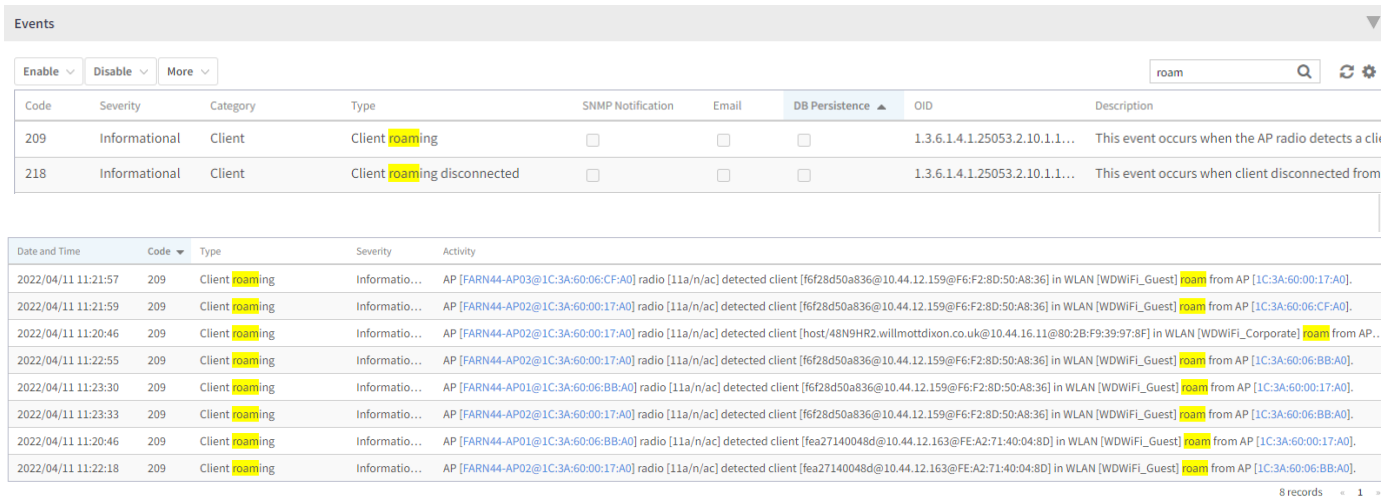
easier roam: sticky → not sticky

The configuration can be changed from the CLI of the SmartZone.

config
domain "Domain Name"
zone "Zone Name"
wlan "WLAN Name"
roam
roam-factor 2.4g x
roam
roam-factor 5g x

Red writing indicates a value that will be unique to your configuration. Note also that the quotes are required for parameters within a partner domain.

Additionally, if you enable DB Persistence event **209/218** on the vSZ you can see the system logs (events) for roaming activity.



Advanced Guide: LDAP Authentication on Ruckus vSZ via Azure AD Domain Services (Azure AD DS)

Since **Ruckus Virtual SmartZone (vSZ) does not support SAML authentication** for admin logins, you must use **Azure AD Domain Services (Azure AD DS)** to provide an LDAP interface that vSZ can authenticate against.

Below is a more detailed breakdown, including user group mappings and troubleshooting.

---

1. Configure Azure AD Domain Services (Azure AD DS) for LDAP

Step 1: Enable Azure AD DS

1. **Log in to Azure Portal**.
2. **Go to "Azure AD Domain Services" (AAD DS)** and create a **managed domain**:
   - Set the **DNS domain name** (e.g., `corp.yourcompany.local`).
   - Choose a **resource group** and **region**.
   - Select an **Azure Virtual Network (VNet)** (Ensure vSZ can reach this network).
3. **Synchronize Users from Azure AD to Azure AD DS**:
   - Azure AD DS automatically synchronizes users and groups from Azure AD.
   - Users must have **Kerberos and NTLM authentication enabled** (this is automatic for synced users).

Step 2: Enable Secure LDAP (LDAPS)

1. **Enable Secure LDAP** under **Azure AD DS > Properties**.
2. **Download and install the SSL certificate** for LDAPS.
3. **Allow LDAP over SSL (TCP 636)** through your **Network Security Group (NSG)**.

Step 3: Verify LDAP Access

1. Run the following command from a machine that can reach Azure AD DS: `ldp.exe`
2. Connect to **`yourdomain.local`** on **port 636**.
3. Bind using an Azure AD DS **admin account**.
4. If successful, LDAP is ready.

---

2. Configure LDAP Authentication on Ruckus vSZ

Step 1: Add an LDAP Server

1. **Log in to vSZ Web UI**.
2. Navigate to **Administration > AAA Servers**.
3. Click **Create** and select **LDAP**.
4. Fill in the LDAP server details:
   - **Server Address**: Enter the **IP Address of Azure AD DS**.
   - **Port**: `636` (for LDAPS).
   - **Bind DN**: A service account in Azure AD DS, e.g.: `cn=admin,ou=Users,dc=yourcompany,dc=local`
   - **Password**: The service account's password.
   - **Base DN**: The starting point for LDAP searches, e.g.: `dc=yourcompany,dc=local`
   - **User Attribute**: `sAMAccountName`
   - **SSL**: **Enable LDAPS**
   - **Certificate**: Upload the LDAPS certificate from Azure AD DS.
5. **Click Test Connection** to verify authentication.

---

3. Configure User Group Mappings

Since Azure AD DS syncs groups from Azure AD, you can **map LDAP groups to Ruckus admin roles**.

Step 1: Find LDAP Group DNs

1. Run **`ldp.exe`** and connect to Azure AD DS.
2. Browse to **OU=Groups** to locate the full **Distinguished Name (DN)** of groups, e.g.: `cn=WiFiAdmins,ou=Groups,dc=yourcompany,dc=local`

Step 2: Assign LDAP Groups in vSZ

1. **Go to "Administration > Users & Roles"**.
2. **Create a new User Group**.
3. **Select "Authentication Type: LDAP"**.
4. **Enter Group DN**, e.g.:
   `cn=WiFiAdmins,ou=Groups,dc=yourcompany,dc=local`
5. Assign appropriate **permissions (e.g., System Admin, Read-Only Admin, etc.)**.
6. **Save and Apply**.

---

4. Troubleshooting LDAP Authentication on vSZ

Issue 1: LDAP Connection Fails

- **Check firewall rules:** Allow **TCP 636** from vSZ to **Azure AD DS**.
- **Verify LDAPS certificate:** Upload it again if necessary.
- **Ensure service account has permissions** to query LDAP.

Issue 2: Users Cannot Log In

- **Confirm correct Base DN:** Run `ldp.exe` to verify the correct structure.
- **Ensure correct user attribute (`sAMAccountName`)** in vSZ settings.
- **Try logging in with UPN (`user@yourdomain.com`)** instead of the username.

Issue 3: Group Mappings Do Not Work

- Use **full group DN** (not just the group name).
- Ensure users are in the **correct group** in Azure AD DS.
- Run `ldapsearch` to manually verify group membership.

Final Thoughts

Using **Azure AD DS with LDAPS** is the best way to integrate Azure authentication with **Ruckus Virtual SmartZone (vSZ)**. With proper **LDAP configuration and group mappings**, you can ensure **secure authentication** and centralized management.

How to Configure and Optimise SmartRoam on vSZ

Introduction

Some clients do not roam even if they are physically moved to a new location. Not all clients have roaming aggressiveness setting to fine-tune roaming. Apple devices are reported to cling to the AP they first learn an SSID on.

In a multi-AP environment, a client will always be looking for the best AP to connect to. It will remain connected to its current AP and roam to an adjacent AP once the signal level falls below a certain threshold. This behavior ensures best possible performance at all times.

To achieve this, a client must be doing background scanning to learn about its environment. Frequency of this background scan can determine the roaming behavior. Certain clients such as Windows clients allow roaming aggressiveness to be tweaked. "High" setting will make the client to perform background scanning more often to learn about available APs to connect. While the "Low" setting will make the client do less frequent scanning. This setting can be found under the wireless adapter properties.

Unfortunately, this tweaking is not readily available for all client types. For example, various smartphones and Apple clients do not provide this setting to encourage roaming.

For these types of clients, it is obvious to look towards infrastructure for help. Ruckus has added firmware support to disconnect a client if its signal falls below the user-definable threshold. This feature is called SmartRoam. With this feature, there will be an explicit disassociate message to kick off the client.

Method

This is a per-SSID setting as illustrated above. "smart-roam" parameter takes values from 1 to 10.
These are called roam factors, and they map to an RSSI value in dB as per the list below:

Mapping of roaming factor, to RSSI.

RSSI threshold (dB) 'roam_rssi_thrlo'	Scale Factor (#) 'roam_factor'
5	1
10	2
15	3
17	4
20	5
23	6
27	7
32	8
40	9
60	10

easier roam: sticky → not sticky

The configuration can be changed from the CLI of the SmartZone.

config
domain "Domain Name"
zone "Zone Name"
wlan "WLAN Name"
roam
roam-factor 2.4g x
roam
roam-factor 5g x

Red writing indicates a value that will be unique to your configuration. Note also that the quotes are required for parameters within a partner domain.

x Defines the roam factor in the table above i.e. 1-10.

Remember to ensure configuration is saved.

Additionally, if you enable DB Persistence event **209/218** on the vSZ you can see the system logs (events) for roaming activity.

