How to Configure User Policies

What is User Policy?

User Policy, as the term suggests, can be applied to network users to govern their network usage. User Policy consists of four parts – Firewall, Privilege, QoS and Specific Routes, each of which has multiple profiles available for setup, and a particular User Policy would take one profile from each of Firewall, Privilege, QoS and Specific Routes, as defined by the administrator (see Figure 1). For example, User Policy 1 will take Firewall profile 1, Privilege profile 2, QoS profile 1 and Specific Routes profile 5. However, it is recommended to use the same profile number (or name if it has been renamed) across to avoid confusion. In these profiles, the administrator can configure a range of settings – from firewall rules, bandwidth control, routing rules to session allowances and so on.

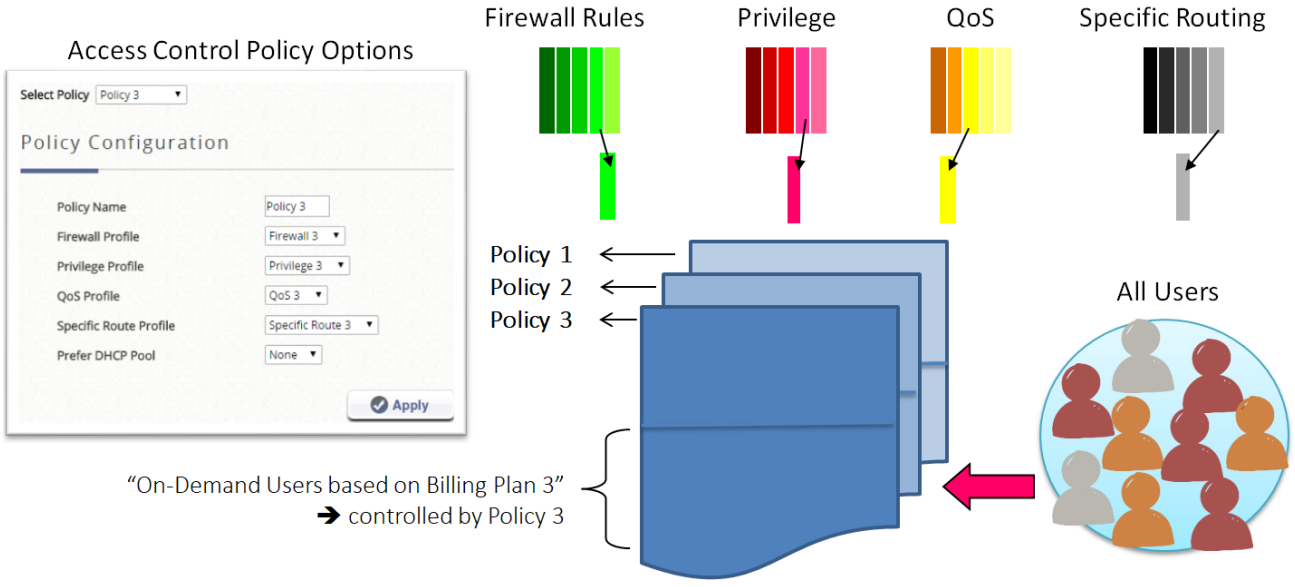

Figure 1

Service Zone Default Policy, Group Policy and Global Policy

User Policy for any user would depend on the Service Zone the user is in, whether this user is placed in a User Group, and the User Group the user is placed into based on the authentication method or account used. All of these factors put together would determine which policy will be applied to a

particular user. See explanations below.

Service Zone Default Policy is the policy enforced on users in a particular Service Zone. This policy is applied to users before they authenticate and also those on the MAC Privilege List that have ready access to the network. This is because before authentication, users are not yet associated with any groups. After authentication, users will be assigned to a Group and no longer be governed by this policy but User Policy, with one exception – those on the MAC Privilege List will still be governed by the Service Zone Default Policy because as these users are not associated with any groups. Note that the Service Zone Default Policy only supports Firewall, Privilege and Specific Routing. An additional note is that users on the IP Privilege List can be assigned to a Group to be governed by a User Policy for a particular Service Zone.

Service Zone → Authentication→ Disable → Service Zone Default Policy

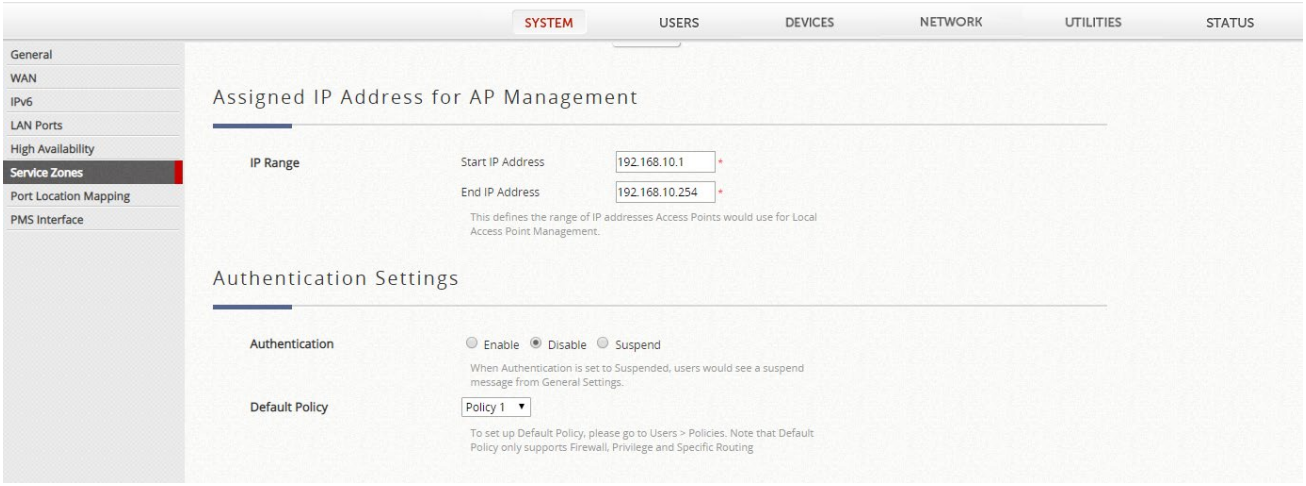

Figure 2

User Group is a set of users that will have the same network access rights, as defined by the network administrator. Grouping can be based on various criteria such as the roles of users at an organization. For example, on any campus, network users can be made up of teaching staff, students and visitors. Therefore, the IT department may set up three User Groups with different network access permissions. On WLAN controllers, depending on the model, there are eight to twenty-four Group profiles available for configuration. Once a user has authenticated, the user will be placed into a group based on the authentication method or account used.

A User Group can be configured to be bound by different Policies for different Service Zones (see Figures 3 and 4). Take the same example of users on a campus, one Service Zone can be setup for

Internet access inside classrooms while another Service Zone can be setup for Internet access in the office area of the teaching staff. So the teaching staff can be bound by one Policy when in classrooms and another Policy when in the office area.

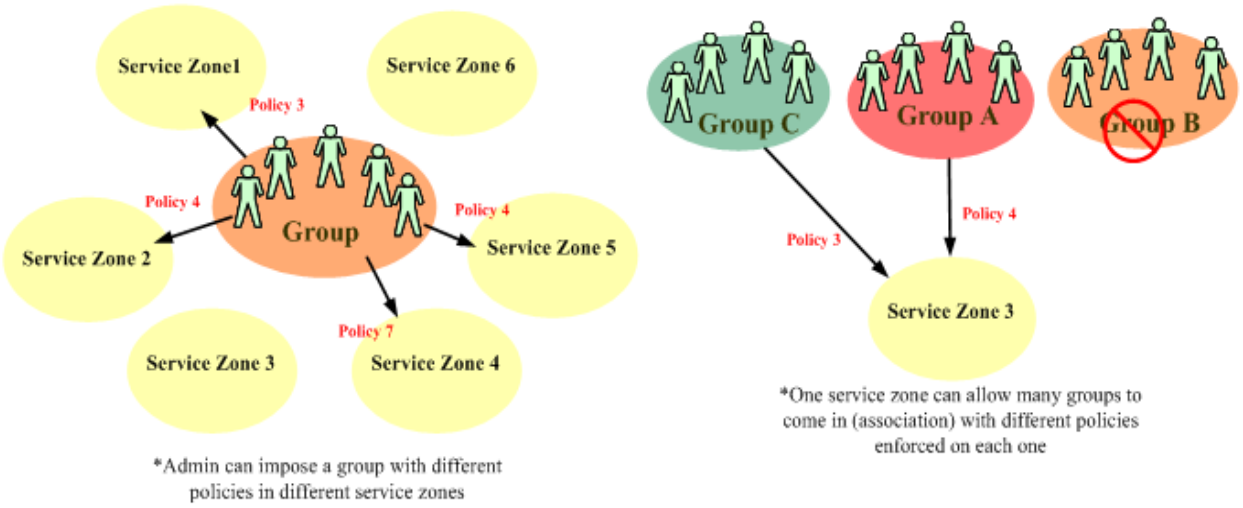

Figure 3

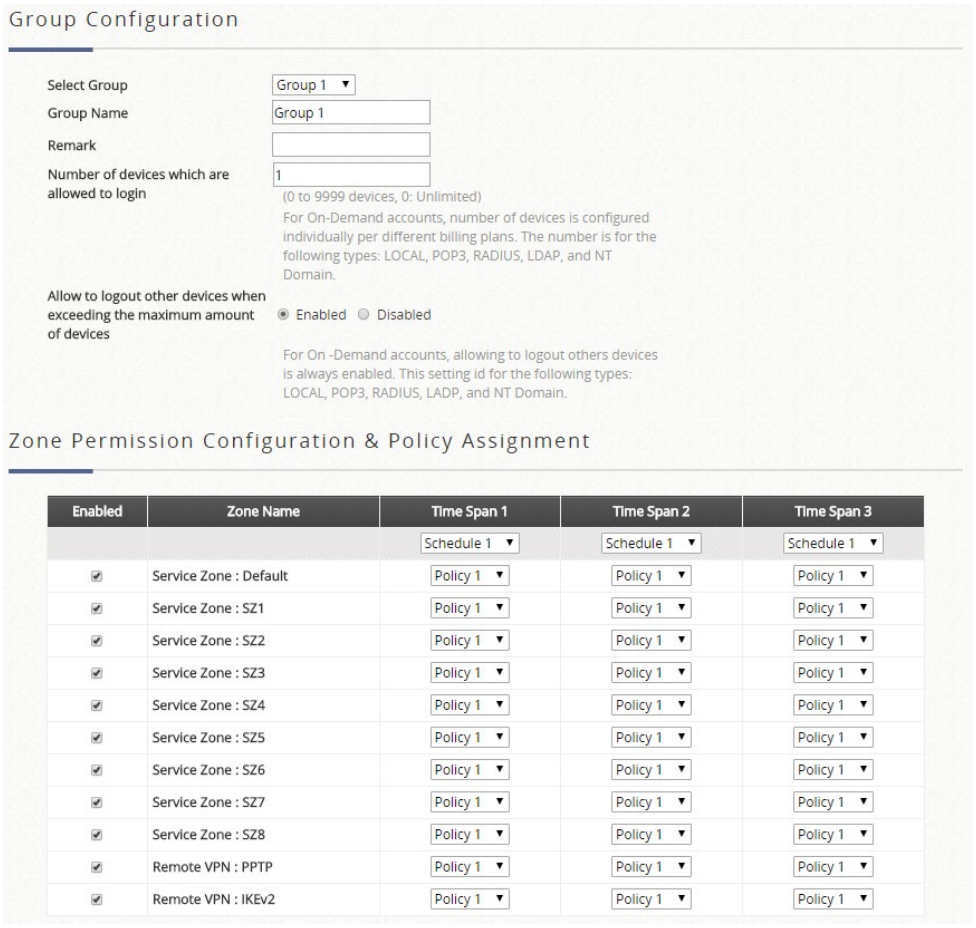

Figure 4

Global Policy is the policy in the background that is applied to all users by default. However, it has a lower priority than Service Zone Default Policy and User Policy, meaning that settings in Service Zone Default Policy or User Policy will overwrite settings in Global Policy if configured.

In summary, the priority of Policy enforcement is Group Policy (Service Zone dependent) > Service Zone Default Policy > Global Policy.

Note: For a client associated to a VAP on a managed access point, where a split tunnel is built from this VAP to a Service Zone on the controller, only Privilege profile can be applied to the client. However, select 802.11ac wave 2 APs additionally supports QoS profile to be applied to the client.

● User Policy Configuration Explained

- **Select Policy:** select the User Policy profile to be configured.
- **Firewall Profile:** select the Firewall profile to be used by this User Policy
  - **Service Protocols**: This link leads to the policy's Service Protocols List page where the administrator can define a list of services by protocol (TCP/UDP/ICMP/IP). The service names defined here form a choice list for configuring firewall rules.
  - **User Firewall Rules**: This link leads to the policy's Firewall Rules page. Rule No. 1 has the highest priority; rule No. 2 has the second priority, and so on. Each firewall rule is defined by Source, Destination, a Service from the policy's Service List, a Pass/Block option and a schedule. The Schedule specifies when the firewall rule is enforced and can be set to Always, Recurring or One Time.
- **Privilege Profile:** select the Privilege profile to be used by this User Policy. The following network privileges can be defined in the profile.
  - **Password Change:** choose "Allow" to give users the flexibility to change their login password

- **Maximum Concurrent Sessions:** a user will be implicitly suspended from any new connection for a fixed time period after the number of their concurrent sessions reaches this threshold
- **Disable timeout for this group:** when enabled, Idle Timeout setting found in Additional Controls > User Session Control will not apply, meaning that users will not be logged out no matter how long they have been idle for. Note that enabling this option may increase the system load

- **QoS Profile:** select the QoS profile to be used by this User Policy. Bandwidth limitations for individuals and groups can be set in the profile. Bandwidth throttling allows the QoS profile to be changed after a certain time period after user authentication. For example, upon initial login, QoS profile 1 is used for User Policy 1, but after 5 minutes, QoS profile 2 will be used for User Policy 1 instead.
  - **Traffic Class:** Each policy can be configured its own traffic class and different Traffic Class Remarking can be set for IPv4 and IPv6 in the same Traffic Profile.
  - **Group Total Downlink:** defines the maximum total downlink bandwidth allowed to be shared by clients within this group.
  - **Group Total Uplink:** defines the maximum total uplink bandwidth allowed to be shared by clients within this group.
  - **Individual Maximum Downlink:** defines the maximum downlink bandwidth allowed for an individual client within this group. Note that this value cannot exceed the value for Group Total Downlink.
  - **Individual Maximum Uplink:** defines the maximum uplink bandwidth allowed for an individual client within this group. Note that this value cannot exceed the value for Group Total Uplink.
  - **Individual Request Downlink:** defines the minimum downlink bandwidth guaranteed for an individual client within this group. Note that this value cannot exceed the value for Group Total Downlink or Individual Maximum Downlink.
  - **Individual Request Uplink:** defines the minimum uplink bandwidth guaranteed for an individual client within this group. Note that this value cannot exceed the value for Group Total Uplink or Individual Maximum Uplink.
- **Specific Route Profile:** select the Specific Route profile to be used by this User Policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this default gateway, which can be WAN1, WAN2 (if any) or a desired IP address.