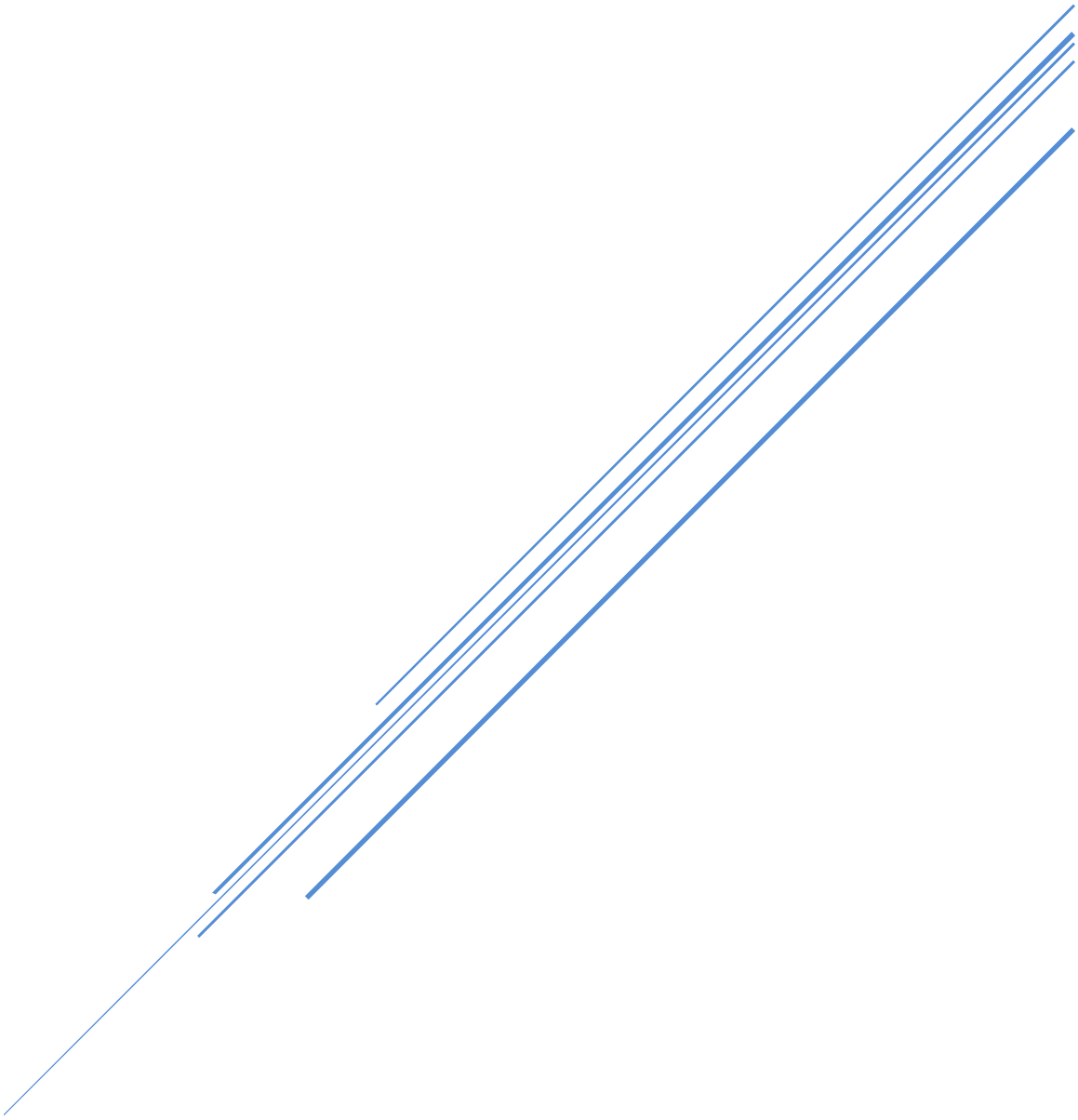
GUEST ACCESS CONFIGURATION

CNPILOT ENTERPRISE APs (E400, E500, ePMP1000 Hotspot)



Cambium Networks

TABLE OF CONTENTS

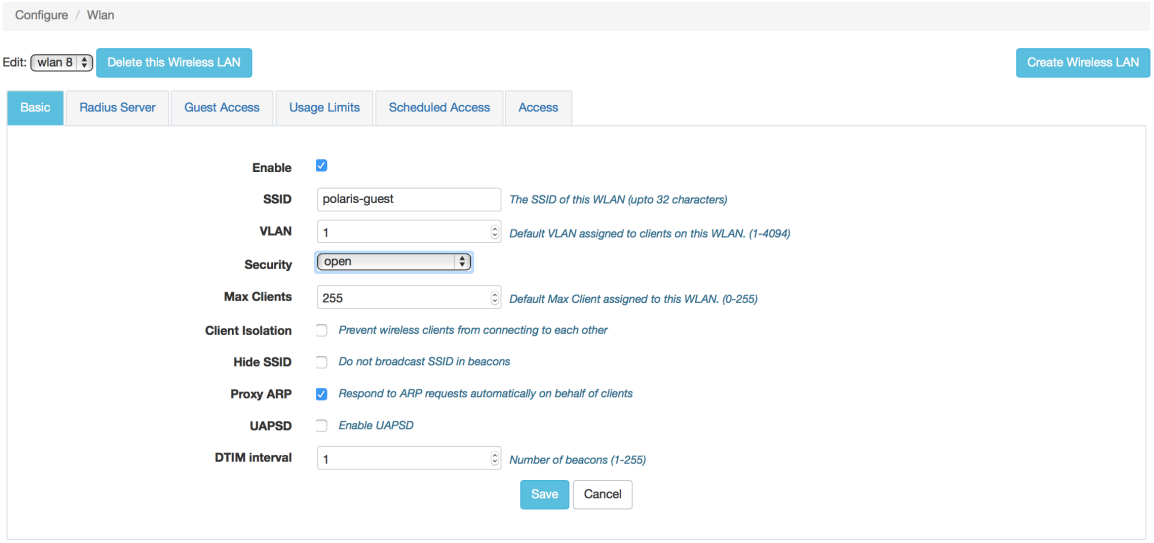
1. Overview

The cnPilot enterprise APs provide powerful, feature-rich Guest Access features that can be used for Public, Enterprise as well as Small-Business deployments of Wi-Fi access. In addition to supporting redirection of users to customized splash pages, multiple authentication mechanisms, as well as accounting, several policy enforcement options give the network administrator the ability to setup their network fine-tuned to their liking.

2. Configuration

Guest Access is configured on a per-WLAN basis. The configuration involves enabling access on an SSID, and configuring a splash page either to be hosted locally on the access point, or on an external server. In the case of an external server, the URL of the server is configured. In the case where the pages are to be hosted locally on the AP, the administrator can customize the login header and text.

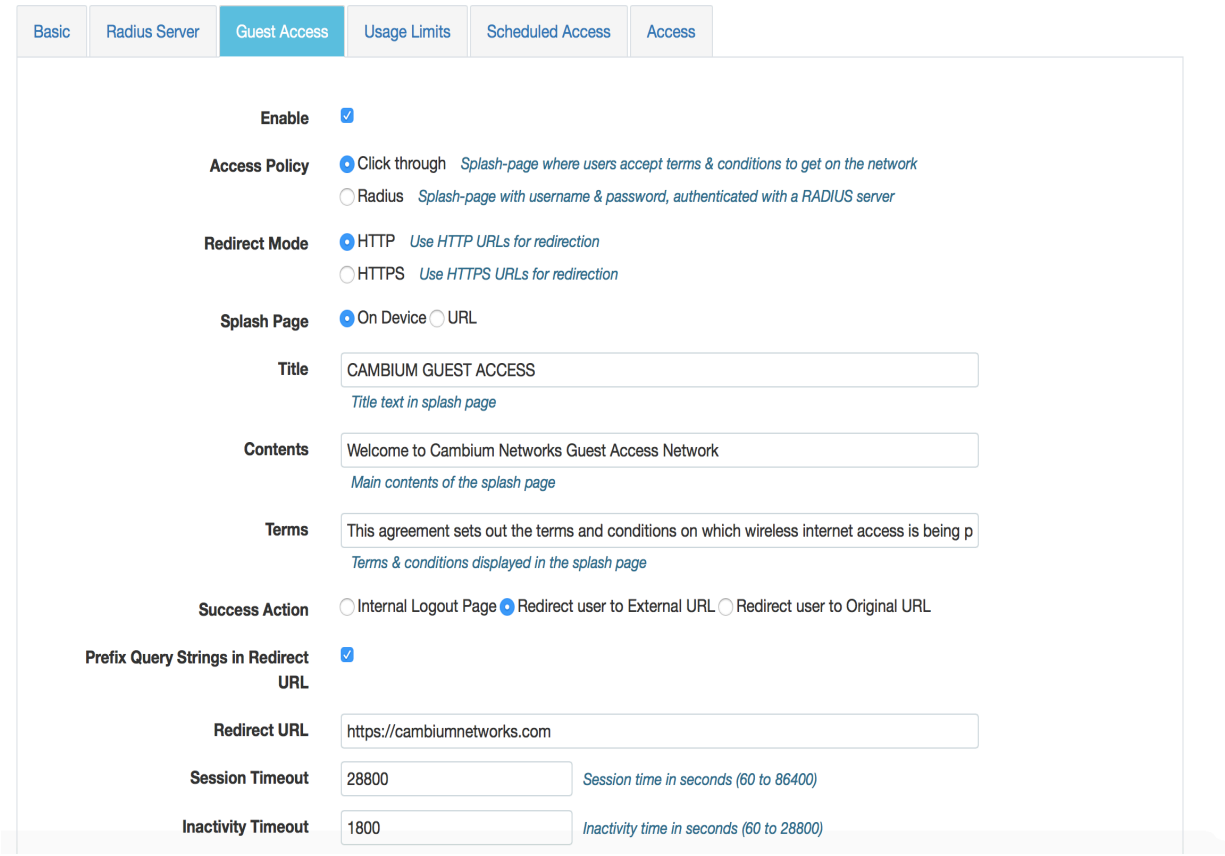
The first step is to create a WLAN (**Configure->WLAN** in GUI) and setup the SSID you wish to use for guest-access



From the CLI this is done as follows:

```
cnWest-5ghz(config)# wireless wlan 1
cnWest-5ghz(config-wlan-1)# ssid polaris-guest
```

After the SSID has been created, guest access can be enabled on it going into Guest Access tab in the same page. In the example below Guest-Access was enabled, and custom text for **Title, Contents** and **Terms** were entered. Also, under the section titled **Success Action** a URL was configured, to which users who successfully connect will be redirected after the splash page.



The same configuration can also be done from the CLI:

```
wireless wlan 1
 ssid Polaris-guest
 guest-access
```

```
 guest-access splash-page title "Cambium Powered Hotspot"
 guest-access splash-page text "Welcome to a Cambium Networks powered
hotspot"
 guest-access splash-page terms-message "This agreement sets out the
terms and conditions on which wireless internet access is being
provided"
 guest-access success-action redirect-url http://cambiumnetworks.com
```

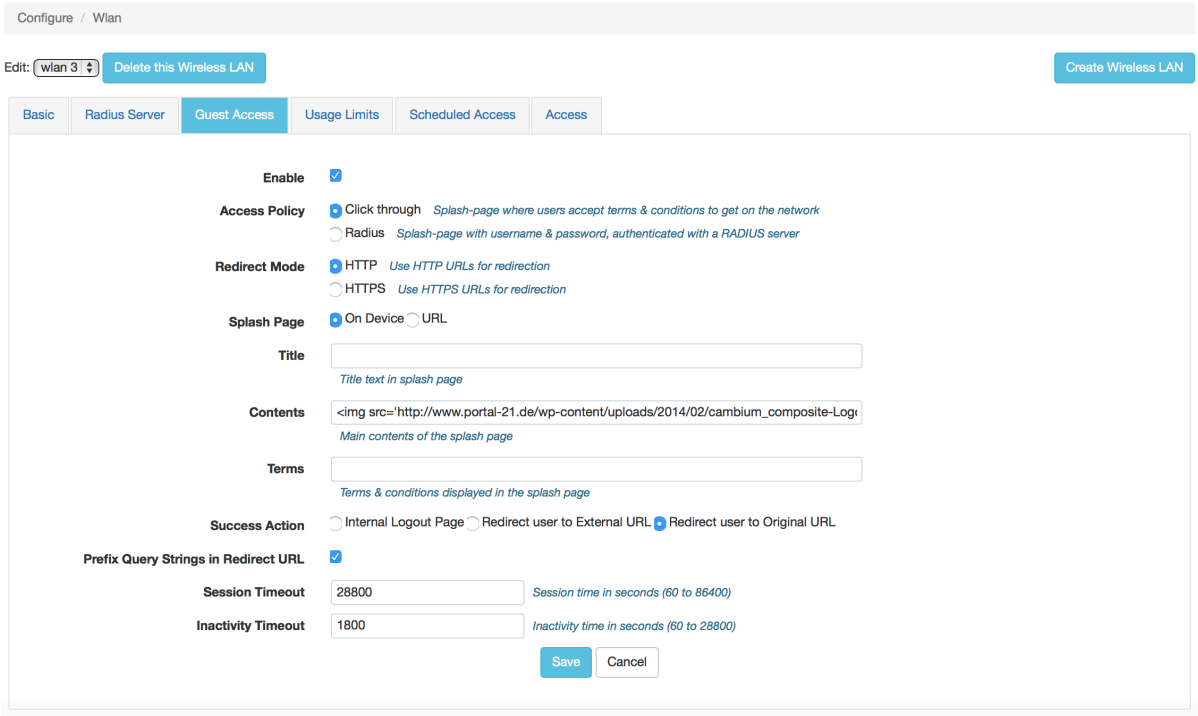
3. Web Page Customization

Customized Logo:

The administrator can customize the Guest Access Web pages by editing the content configuration in UI and the 'text' in guest-access splash-page configuration in UI. A user can embed html tags in the input values of these configurations and can also insert customized logo as an external image. If an external logo or anything which refers to an external URL then that external URL server has to be added in the walled-garden configuration which is the whitelist configuration in the CLI.

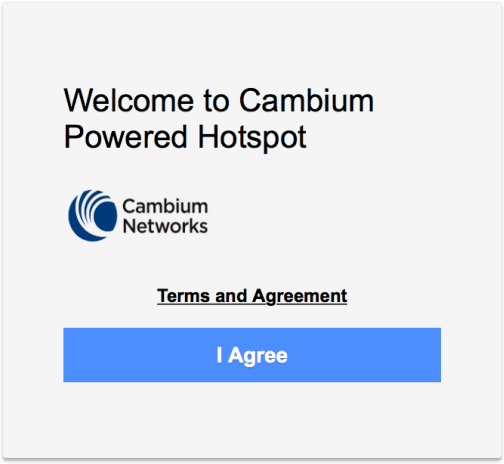
Example CLI/UI configuration which inserts cambium Networks logo in the guest access splash page:

UI:



```
CLI:
 (config-wlan-1)#guest-access splash-page text "<img
src='http://www.portal-21.de/wp-
content/uploads/2014/02/cambium_composite-Logo.png'
style='width:100px;height:50px;'>"
 guest-access whitelist www.portal-21.de
```

Example splash page with Cambium Networks logo:



Customized Terms and Conditions:

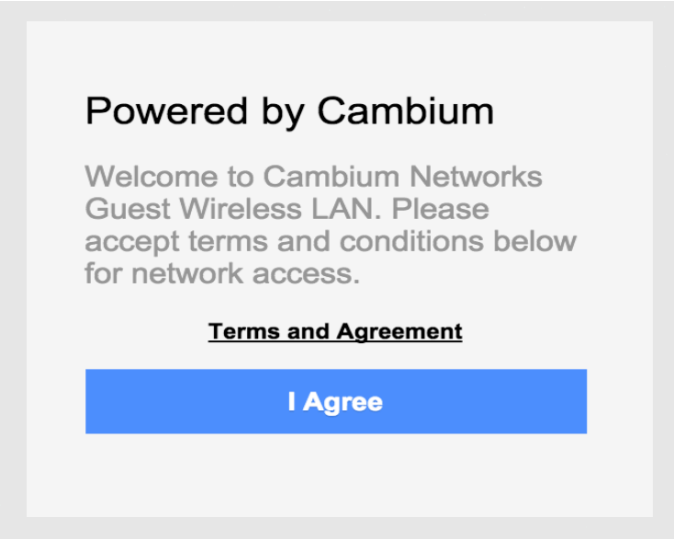
If a user desires to upload customized terms and conditions content which is quite large and can't be accommodated in the regular CLI/UI configuration of guest-access splash-page terms-message then he can upload a terms and condition content file on the access point and the same will be sent to the login splash pages. Currently this configuration is available through CLI only. If multiple WLAN's are using guest access then the terms and condition will be common to them if the terms and condition file has been copied to the access point. One can use delete command to remove this file.

```
CLI:
(config)#import guest-access terms-conditions <path>
path :a TFTP or FTP server path (Eg: tftp://1.2.3.4/terms.txt,
ftp://user:pass@1.2.3.4/terms.txt)
(config)# delete guest-access terms-conditions
```

4. User Authentication

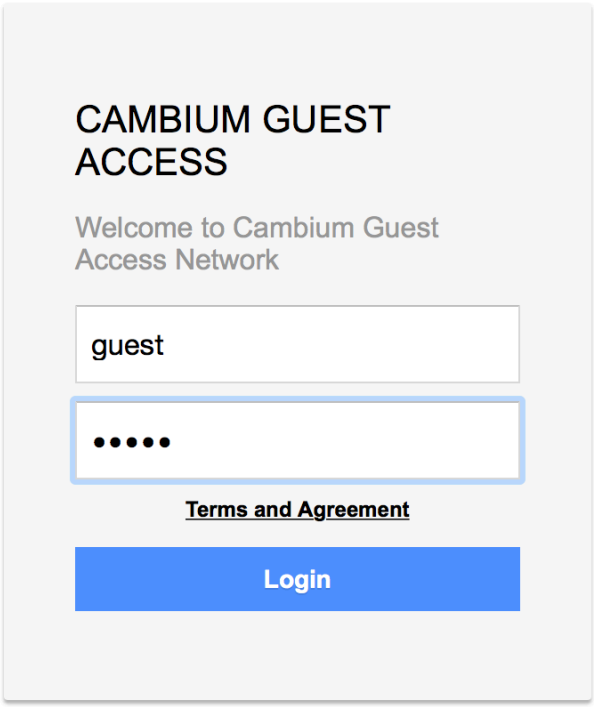
The users accessing the guest network can gain access in one of two ways:

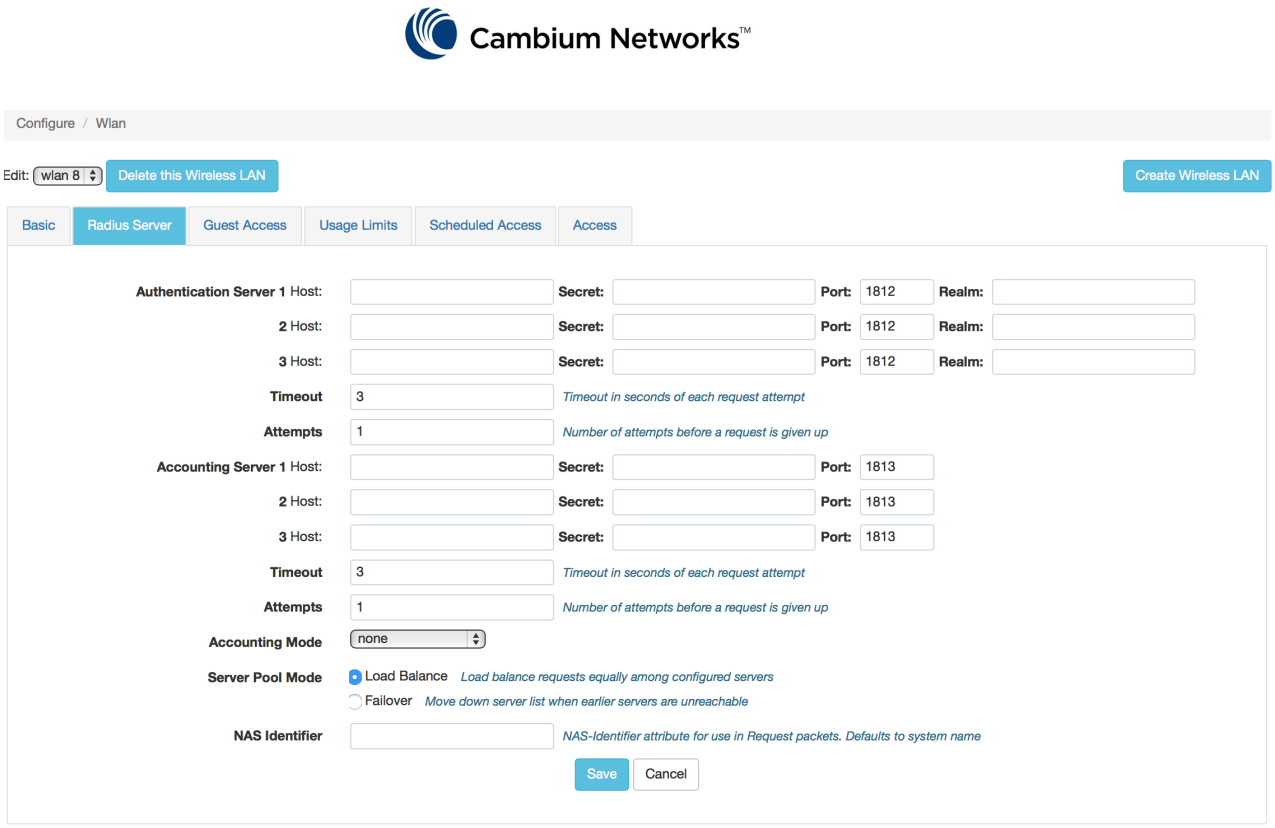
- **ClickThrough** – in this mode of access the user is presented with a splash-page that contains terms and conditions for accessing the network and if the user clicks Accept, then they are on the network and further network access requests are serviced without being redirected.



- **Radius** – in this mode of access the user is presented with splash page that includes text boxes for the user to enter a username and a password. This username and password is then looked up against a RADIUS server, and only if the RADIUS server responds with an Access-Accept, the user is granted network access. The Authentication server must be configured under the **RADIUS Server** TAB of the WLAN configuration page. One can also enable RADIUS accounting for the wireless clients under the same RADIUS Server tab. A user can configure maximum three RADIUS Authentication and Accounting Server. The default Accounting mode is none which means the accounting is disabled and the user can configure either being "start-stop" or "start-interim-stop" mode. The RADIUS Server host address

can be an IP address or a host name. One can also configure RADIUS realm that is used to match the username in the RADIUS authentication request and select the matching RADIUS server. Realm based RADIUS request routing helps to forward authentication requests to relevant authentication servers. The matching is done for realm as a prefix or a suffix to the given username and then selected RADIUS server is used, the same selected RADIUS server index entry is used for the RADIUS accounting server too hence the RADIUS Accounting Server always tries to follow the same index entry as used for RADIUS Authentication Server.





5. Policy Enforcement

In addition to granting access to the network, the administrator can also choose to control and manage the access that has been given to the user. Some of these access policy related features include:

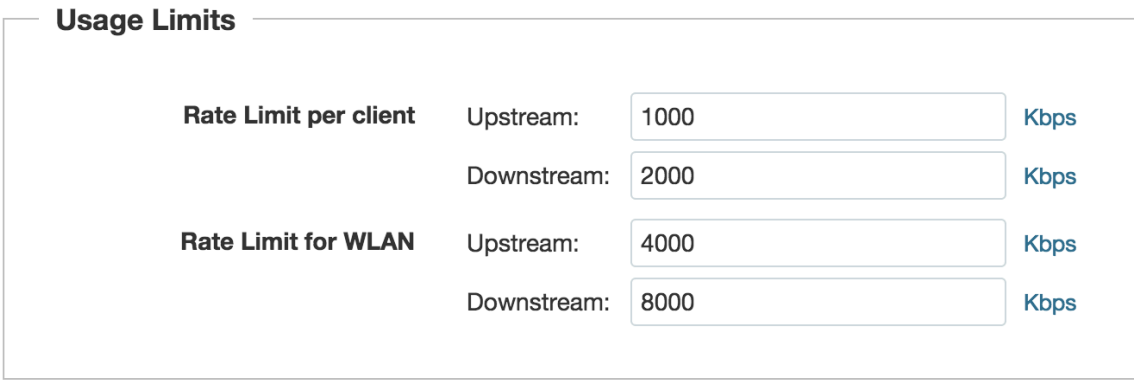
Access Control List: Using ACLs configured under WLAN or Ethernet interface, the administrator can control the access the user gets to various servers and protocols on the network.

```
AP(config-wlan-1)# acl permit ip
acl permit ip PRECEDENCE (SOURCE-IP|any) (DESTINATION-IP|any)
(in|out|any)

Eg: acl permit ip 255 any any any
```

Domain Name Service ACL: By specifying DNS entries that are either permitted or denied, the administrator can choose to allow or block access to certain types of sites. This can be used for instance to block access to Hulu or Netflix or other streaming sites if the deployment has a constricted WAN bandwidth.

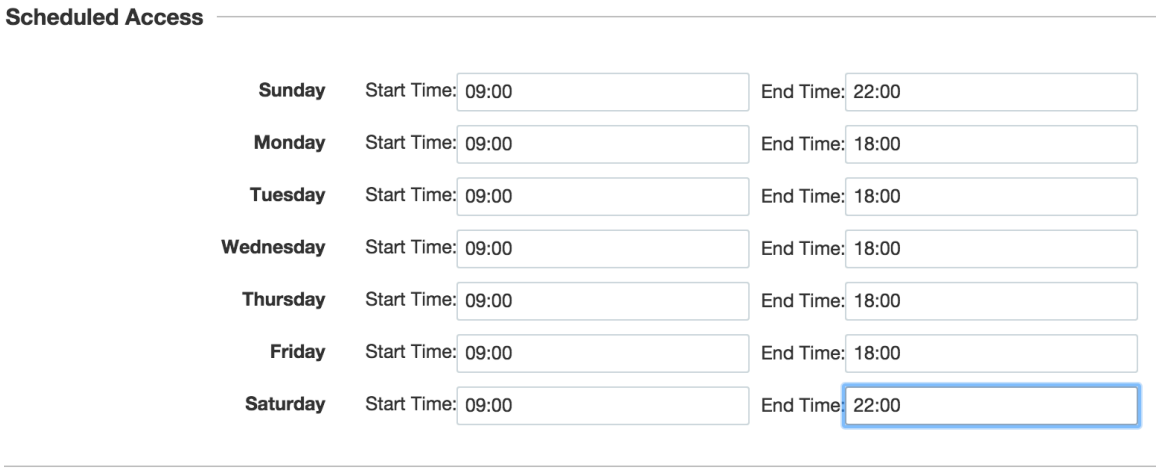
```
AP(config-wlan-1)# dns-acl deny 1

  [DOMAIN] [PRECEDENCE]. Where domain can include wildcards (Eg:
*.cambiumnetworks.com)
    and PRECEDENCE is <1-256>


Eg: AP(config-wlan-1)# dns-acl deny 1 *.netflix.com
```

Rate Limit: The administrator can choose to restrict the maximum bandwidth a client or a particular WLAN as a whole might use on the access point. These can be configured from the CLI or the GUI as follows:




```
cnWest(config-wlan-1)#rate-limit client 10000
```

Scheduled Access: In addition to the other options above the administrator can choose to setup a certain time during which access is allowed. This schedule could either be at a certain time everyday, or customized to each day of the week. It can be configured in the CLI and GUI as follows:




```
cnWest(config-wlan-1)#scheduled-access Monday 09:00-18:0
```

6. Walled Garden

In certain scenarios the administrator may want to provide access to some websites even to clients that have not yet completed authentication. This could be the website of the host, or a payment gateway. Such a walled garden site can be configured as follows:

```
cnWest(config-wlan-1)#Guest-access whitelist 192.168.0.44

cnWest(config-wlan-1)#Guest-access whitelist cambiumnetworks.com
```