

Let's start creating a new Access List

Edit Access List ✕

[Details](#) [Authorization](#) [Access](#)

Name *

Satisfy Any Pass Auth to Host

Cancel Save

Create one or more username/password for the ACL.

Edit Access List ✕

[Details](#) [Authorization](#) [Access](#)

Basic Authorization via [Nginx HTTP Basic Authentication](#)

Username	Password
<input type="text" value="opensprinkler"/>	<input type="password" value="o*****"/>

Add

Cancel Save

Now, we need to create the Proxy Host for OpenSprinkler.

Edit Proxy Host [X]

Details Custom locations SSL Advanced

Domain Names *

internet.address.org

Scheme * http **Forward Hostname / IP *** opensprinkler.lan.ip **Forward Port *** 8080

Cache Assets Block Common Exploits

Websockets Support

Access List

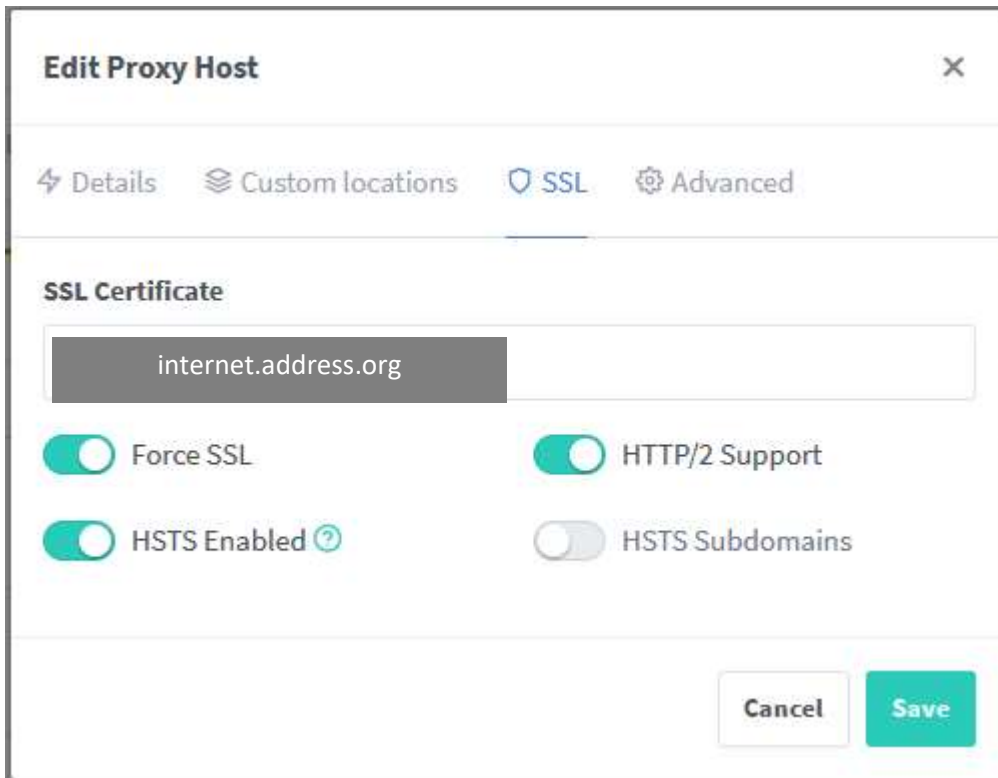
OpenSprinklerACL

Cancel Save

Insert your own internet host FQDN as “Domain Names” and your OpenSprinkler LAN IP address as “Forward Hostname/IP”.

Select the previously created Access List and “Block Common Exploits” to improve security.

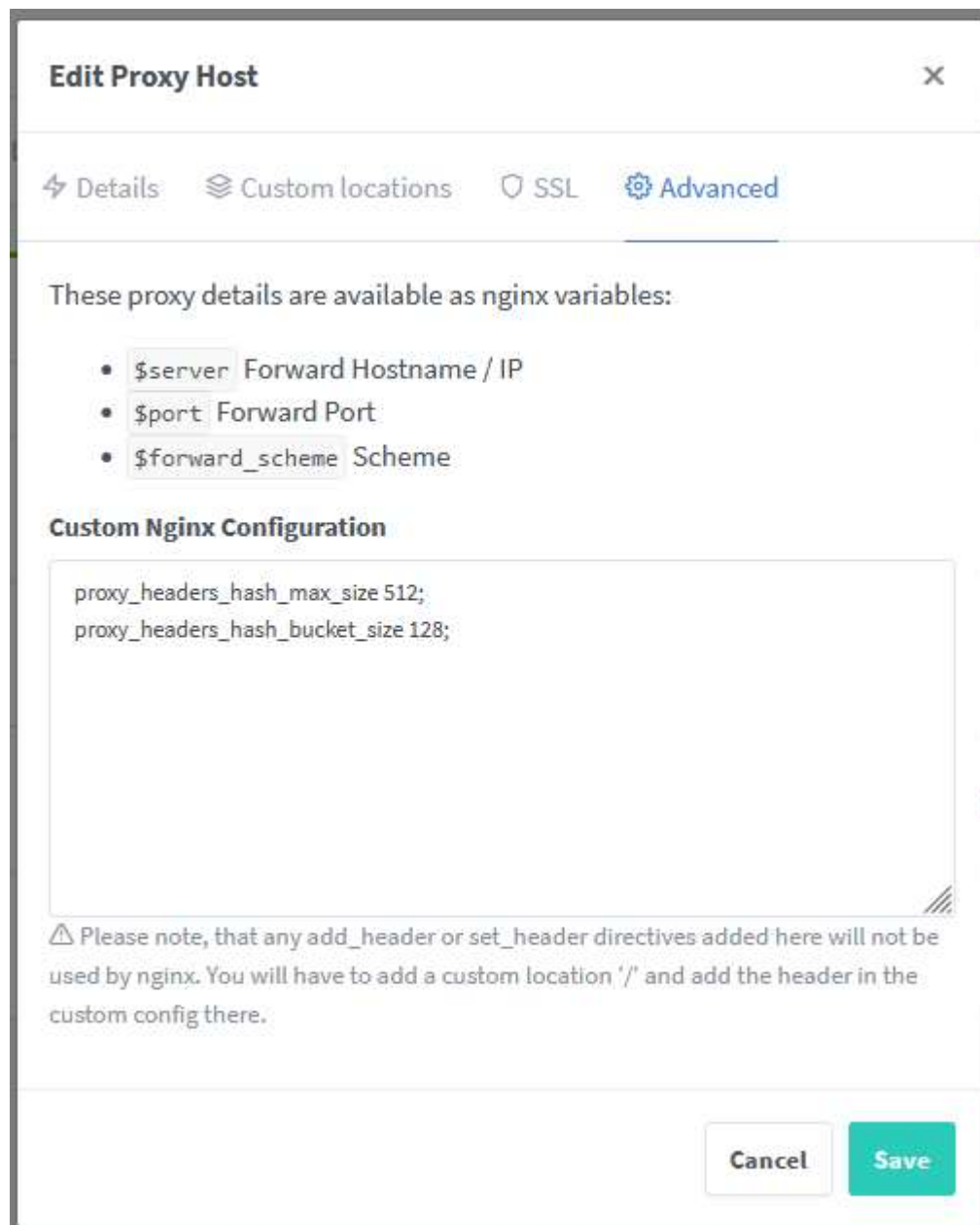
Configure SSL. The interface should be quite different, I am taking screenshot of the editing of an existing host.



Leaving the configuration this way you will be able to access OpenSprinkler through a web browser, but the mobile app should fail. We need to add an advanced configuration to fix it.

Go to the Advanced tab and insert this two lines:

```
proxy_headers_hash_max_size 512;  
proxy_headers_hash_bucket_size 128;
```



The screenshot shows a dialog box titled "Edit Proxy Host" with a close button (X) in the top right corner. Below the title bar, there are four tabs: "Details", "Custom locations", "SSL", and "Advanced". The "Advanced" tab is selected and highlighted. Below the tabs, the text reads "These proxy details are available as nginx variables:" followed by a bulleted list:

- `$server` Forward Hostname / IP
- `$port` Forward Port
- `$forward_scheme` Scheme

Below the list is a section titled "Custom Nginx Configuration" with a text area containing the following code:

```
proxy_headers_hash_max_size 512;  
proxy_headers_hash_bucket_size 128;
```

At the bottom of the text area, there is a warning icon and the text: "Please note, that any add_header or set_header directives added here will not be used by nginx. You will have to add a custom location '/' and add the header in the custom config there."

At the bottom right of the dialog box, there are two buttons: "Cancel" and "Save".

One step more...

Go to the Custom Location tab and create the custom location “/”.

Click on the gear icon on the right and insert this code:

```
if ($request_method = "OPTIONS") {  
    add_header Access-Control-Allow-Origin $http_origin;  
    add_header Access-Control-Allow-Methods $request_method;  
    add_header Access-Control-Allow-Headers $http_access_control_request_headers;  
    return 204;  
}
```

Edit Proxy Host [X]

Details Custom locations SSL Advanced

Add location

Define location *

location / [gear icon]

Scheme * http **Forward Hostname / IP *** opensprinkler.lan.ip **Forward Port *** 8080

Add a path for sub-folder forwarding.
Example: 203.0.113.25/path/

```
if ($request_method = "OPTIONS") {  
    add_header Access-Control-Allow-Origin $http_origin;  
    add_header Access-Control-Allow-Methods $request_method;  
    add_header Access-Control-Allow-Headers  
$http_access_control_request_headers;  
    return 204;  
}
```

Delete

Cancel Save