

# System Admin - Port Management

- Overview
- Logging in
- Settings
  - Changing Ports
  - LetsEncrypt
  - Disabling a Service
  - Configuring HTTPS
  - Secure Provisioning

## Overview

This page allows you to set port numbers for increased security.

## Logging in

- On the top menu click **Admin**
- In the drop down click **System Admin**
- In the right side navigation box click **Port Management**

## Settings

### Port Management

This allows you to set port numbers for various services. The available ports you can configure are as follows:

- Admin - Administration for this system (This interface). Default port 80. (Can not be disabled)
- UCP - User Control Panel. Default port 81
- HTTP Provisioning - Access to provisioning files. Default port 84
- RESTful API - Default port 83
- RESTful Phone Apps - Default port 82
- LetsEncrypt - Only allows access to LetsEncrypt tokens. Should be on port 80

Note that **all http ports** provide access to /.well-known (which is used by LetsEncrypt to validate certificates) in addition to their normal use. However, as LetsEncrypt requires that this be present on port 80, the LetsEncrypt port **only** permits access to /.well-known and nothing else.

Service Name	Insecure Port (http)	Secure Port (https)
Admin	Port 8080	Port 1443
UCP	Port 81 (Default)	Port 443
HTTP Provisioning	Port 84 (Default)	Port 2443
RESTful API	Port 83 (Default)	Port 3443
RESTful Phone Apps	Port 82 (Default)	Port 4443
LetsEncrypt	Port 2134	HTTP Only

This machine has Sysadmin Pro activated, which gives you the ability to password-protect HTTP and HTTPS provisioning requests.

Secure Provisioning is enabled on both HTTP and HTTPS ports (defined above), with the username 0e351a4e and password d07ef38ad0e35982

You can configure Authentication settings in the **Provisioning Protocol** section of Sysadmin Pro

Port	Default Port #	Function
<b>Admin</b>	80	Web port controlling the system
<b>UCP</b>	81	User Control Panel
<b>HTTP Provisioning</b>	84	Access to provisioning files

<b>RESTful API</b>	96	Access to RESTful API
<b>RESTful Phone Apps</b>	88	Access to RESTful Phone Apps
<b>LetsEncrypt</b>	80	Only provides access to LetsEncrypt required files

## Changing Ports

To change any of the ports, you can use the dropdown to select a port number, or pick 'Custom Port' to select your own. When complete, click the **Update Now** button. Your changes will take effect immediately.

## LetsEncrypt

The LetsEncrypt service returns an error when any file is requested, apart from files required by LetsEncrypt for certificate generation/renewal. This allows you leave port 80 exposed to the outside world, without concern that any other services are potentially exposed. When any file is request, the request will return a 'Permission Denied'. LetsEncrypt **only** works over HTTP, not HTTPS, which is why the 'HTTPS' port is disabled.

## Disabling a Service

To disable a service inside Apache, set the port to be **Disabled**

## Configuring HTTPS

HTTPS is only available when you have assigned a SSL Certificate to the machine through the HTTPS Setup page. You will not be able to assign ports until that is complete.

## Secure Provisioning

Please note that [Secure Provisioning](#) is only available when Sysadmin Pro is activated on the server.