|  |
| --- |
| **JDN Standards – Aruba IAP** |

Introduction 2

Available WiFi networks 3

Switch setup 5

Preparation 5

Configuration 5

Virtual controller setup 6

Preparation 6

Configuration 6

Manual Configuration 7

leisure.\*\*.situs 7

Add user for authentication wifilocal.\*\*.situs 10

Configuring individual AP’s 11

Zones: 11

Configuration 11

Whitelisting the MAC address of a barcode scanner 12

RADIUS - Allowing access to the VPN to JDN devices 13

# Introduction

This document describes the technical wifi setup of the standards as defined for JDN deployments in 2018, Standards version 1.1. This document is specific to JDN ships & remote sites and should not be seen as relevant for head offices.

Dell IAPs are "controllerless" in the sense that they are able to run on a virtual controller which is present inside each access point. One "master" is elected based on which has booted first. The other IAPs synchronize their configuration from the master, meaning that after configuring the first access point, the others are plug & play.

Note that this can lead to a dangerous situation if an access point without configuration is booted before those which already have a configuration. The other IAPs will be reset to a blank config if they are powered on after the other IAP.

A downside of using the virtual controllers, is that only one captive portal can be created. A physical controller does not have this limitation.

The access points can be converted to use a physical controller instead of the built-in virtual controller. For this one or more physical controllers are required, as well as the necessary software licenses.

# Available WiFi networks

Each type of site has different types of networks available:

* **Vessel:**
  + **admintrust.\*\*.situs**: For handscanner use only
    - **Enabled** & Hidden
    - WPA-2 Personal
    - Native VLAN (900)
    - **MAC white listing**
  + **crewdia.\*\*.situs**: For use in emergencies
    - **Disabled**
    - WPA-2 Personal
    - VLAN 901
  + **crewlan.\*\*.situs**: For use in emergencies
    - **Disabled**
    - WPA-2 Personal
    - VLAN 905
  + **guest.\*\*.situs**: For use by clients & partners
    - **Enabled**
    - WPA-2 Personal
    - VLAN 904
  + **wifilocal.\*\*.situs**: For recreational use bycrew
    - **Enabled**
    - WPA-2 Personal
    - **Captive portal** (30 minute reauth)
    - VLAN 906
  + **leisure.\*\*.situs**: For recreational use bycrew
    - **Enabled**
    - WPA-2 Personal
    - VLAN 304
* **Site:**
  + **admintrust.\*\*.situs**: For handscanner use only
    - **Enabled** (if handscanners are used on-site) & Hidden
    - WPA-2 Personal
    - Native VLAN (900)
    - **MAC white listing** (handscanner MAC only)
  + **adminuntrustdata.\*\*.situs**: For use with JDN equipment only
    - **Enabled**
    - WPA-2 Personal
    - VLAN 901
  + **adminuntrustvoice.\*\*.situs**: For voice related applications
    - **Disabled**
    - WPA-2 Personal
    - VLAN 905
  + **guest.\*\*.situs**: For use by clients & partners
    - **Enabled**
    - WPA-2 Personal
    - VLAN 904
* **Remote JDN Site (Integrated Jan de Nul):**
  + **REMOTE\_RF\_DATA**: For use with JDN equipment only
    - **Enabled**
    - WPA-2 Enterprise
    - **RADIUS** authentication to JDN domain
    - VLAN 901
  + **XXX\_GUEST**: For use with JDN equipment only

(XXX = site id, example ZEL\_GUEST)

* + - **Enabled**
    - WPA-2 Personal
    - VLAN 904 Static

# Switch setup

## Preparation

Identify all the ports you want to use as Aruba uplink port.

## Configuration

Use the commands below to configure an Aruba uplink on a POE switch.

Example: ge-\*/0/\*\* -> ge-2/0/47

First make sure that all your VLANs of the port you want to configure are gone:

del interfaces ge-\*/0/\*\* unit 0 family ethernet-switching

del vlans admin-untrust-data interface ge-\*/0/\*\*.0

For vessels:

set interfaces ge-\*/0/\*\* description "ARUBA TRUNK"

set interfaces ge-\*/0/\*\* unit 0 family ethernet-switching port-mode trunk

set interfaces ge-\*/0/\*\* unit 0 family ethernet-switching vlan members guest

set interfaces ge-\*/0/\*\* unit 0 family ethernet-switching vlan members crew-lan

set interfaces ge-\*/0/\*\* unit 0 family ethernet-switching vlan members crew-dia

set interfaces ge-\*/0/\*\* unit 0 family ethernet-switching vlan members wifi-local

set interfaces ge-\*/0/\*\* unit 0 family ethernet-switching vlan members leisure

set interfaces ge-\*/0/\*\* unit 0 family ethernet-switching native-vlan-id 900

set protocols rstp interface ge-\*/0/\*\*.0 mode point-to-point

set poe interface ge-\*/0/\*\* priority high

For sites:

set interfaces ge-\*/0/\*\* description "ARUBA TRUNK"

set interfaces ge-\*/0/\*\* unit 0 family ethernet-switching port-mode trunk

set interfaces ge-\*/0/\*\* unit 0 family ethernet-switching vlan members guest

set interfaces ge-\*/0/\*\* unit 0 family ethernet-switching vlan members admin-untrust-data

set interfaces ge-\*/0/\*\* unit 0 family ethernet-switching vlan members admin-untrust-voice

set interfaces ge-\*/0/\*\* unit 0 family ethernet-switching native-vlan-id 900

set protocols rstp interface ge-\*/0/\*\*.0 mode point-to-point

set poe interface ge-\*/0/\*\* priority high

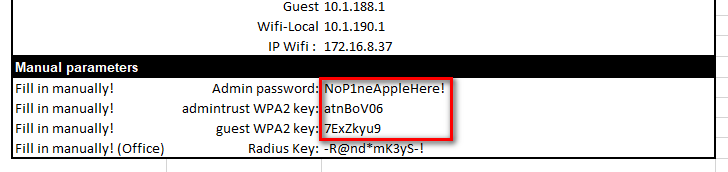
**Warning:** Never manually add "*unit 0 family ethernet-switching vlan members* ***admin-trust***" to the VLAN trunk presented to the access points! Since admin-trust (vlan 900) is already the native-vlan, it does not need to be added separately. Doing so will cause packet drops an eratic behavior.

# Virtual controller setup

## Preparation

Use one access point to make your configuration. When the configuration is finished you can plug in the other AP’s that will download their config from the master AP.

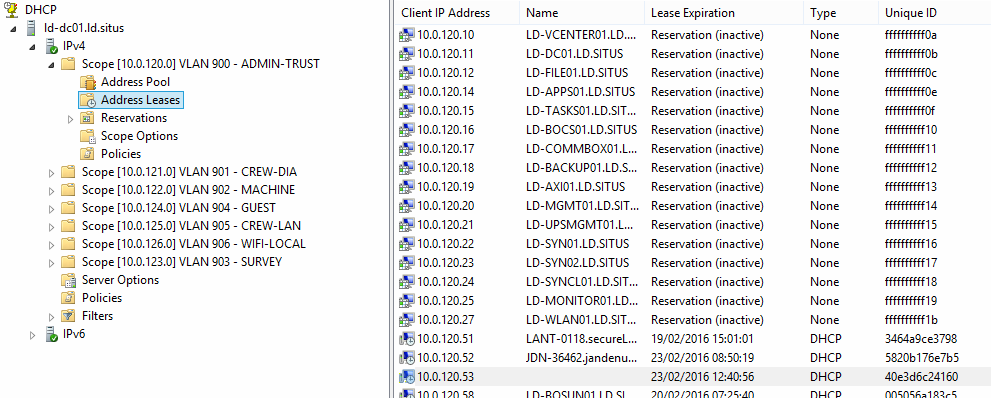
Open the excel sheet **Aruba-Dell-IAP.xlsx** to generate the configuration for your IAP(s), found in \\Jdn-file01\ict\_new\_standard\_sites\_vessels\Scripted Install\Aruba-Dell IAP (Standaarden 1.1). Edit the Manual parameters section as below:



Choose the tab in accordance to your setup type and copy the entire configuration to a temporary .txt file.

\\jdn-file01\homes$\INF152LDW\ARUBA.png

## Configuration

When the AP is booted, you will notice it will start broadcasting an "instant" SSID. You will also find a DHCP lease in the ADMIN-TRUST DHCP scope. You can double check with its mac address.

Start Putty and connect to the IP address of the IAP through SSH.

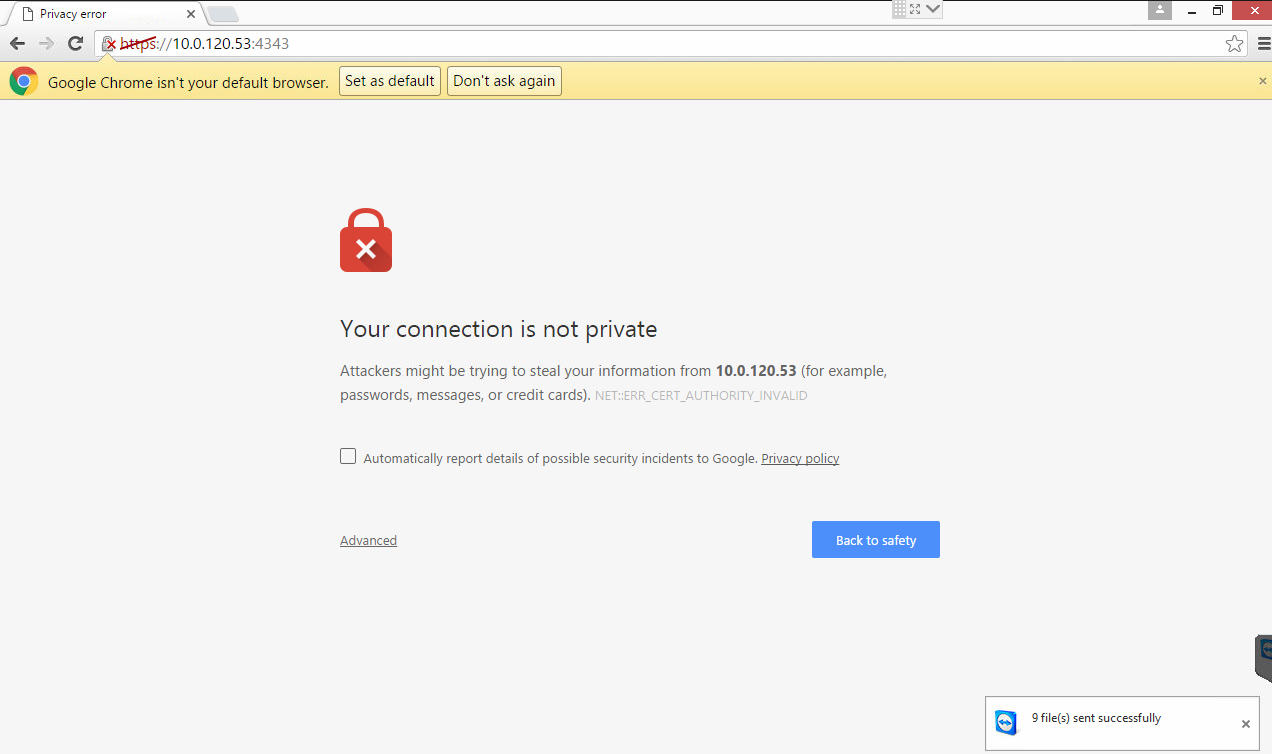
Log in with username admin and password admin and paste the previously generated config from your .txt file.  
If this is completed, you will receive the result as below:

\\jdn-file01\homes$\INF152LDW\ARUBA_2.png

# Manual Configuration

After the configuration is applied, you still need to apply some settings manually.

Use Google Chrome to browse to the IP address of the AP

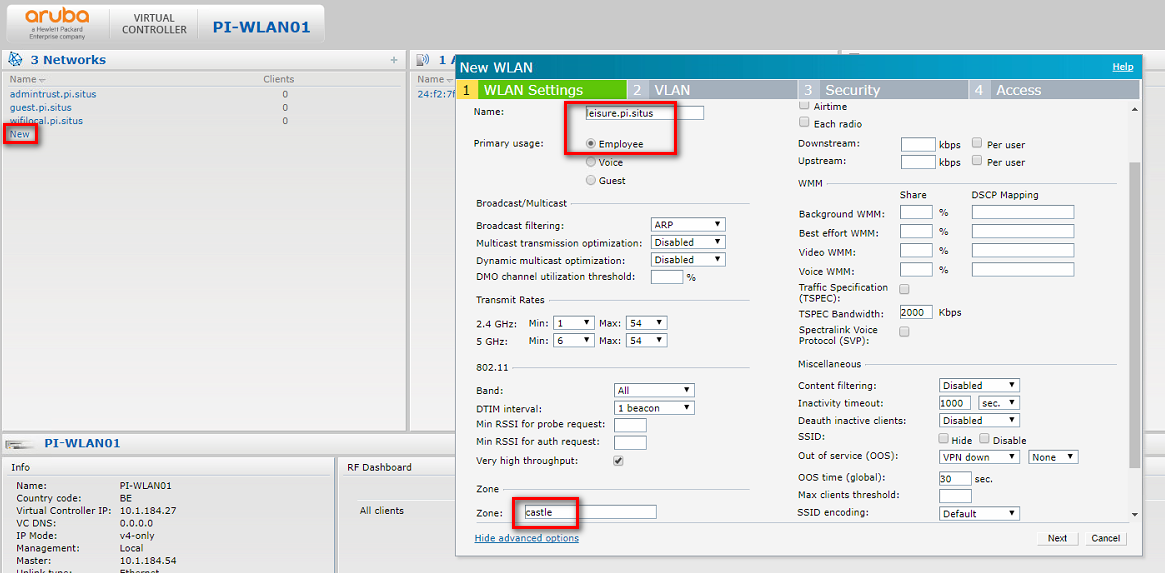


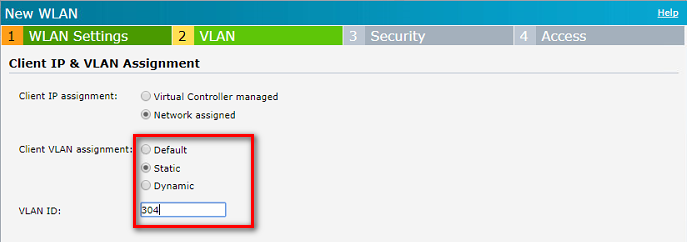
Login with the admin credentials

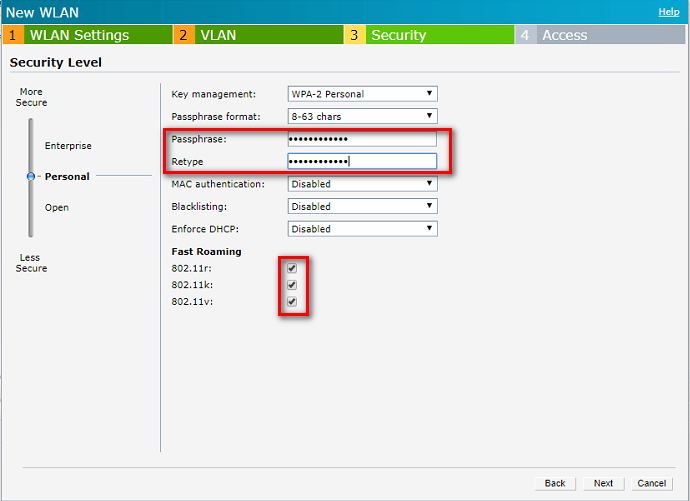
Click New the Networks panel and add the leisure SSID.

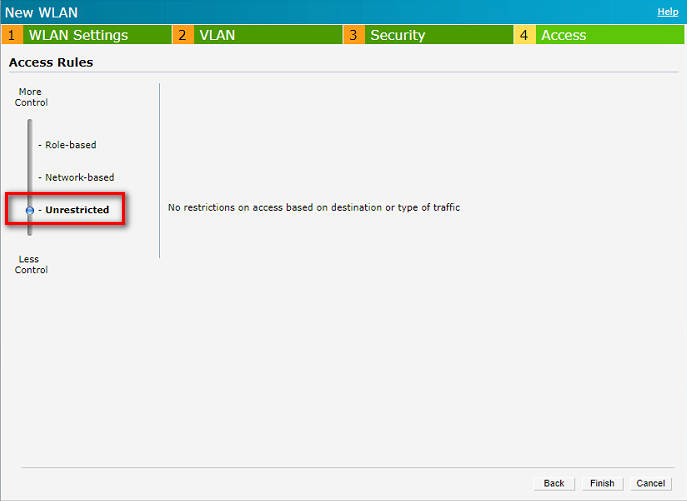
### leisure.\*\*.situs

* Name SSID: leisure.\*\*.situs
* Primary usage: employee
* Client VLAN assignment: Static
* VLAN ID: 304
* Zone: castle
* Fast roaming: ON

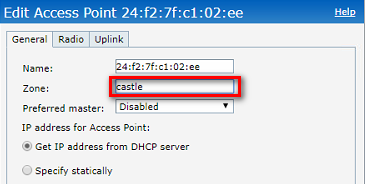








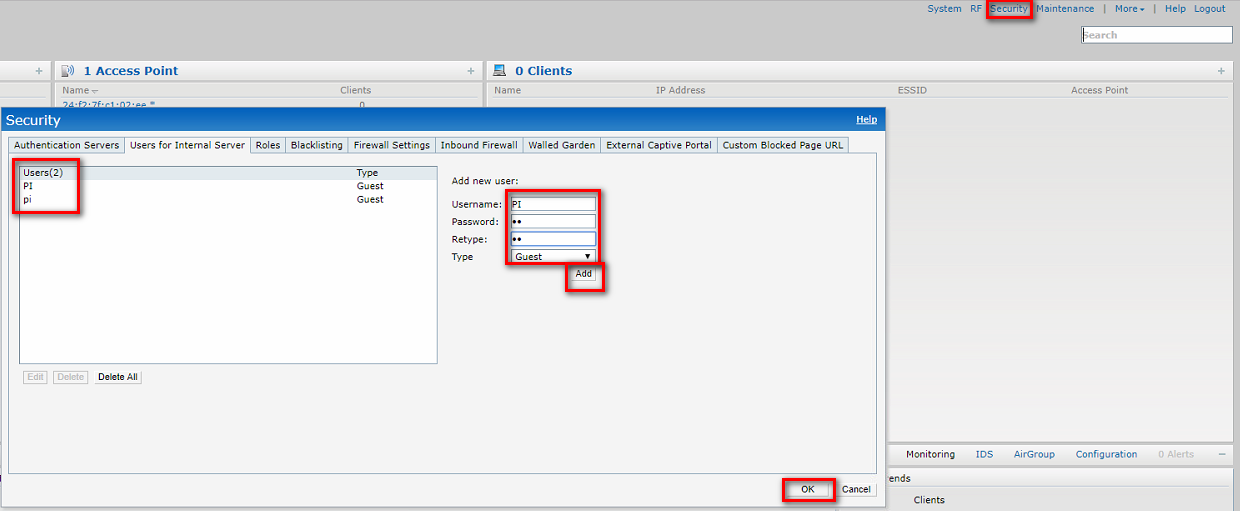
Don’t forget to set your Zone on the IAPs to castle (even when using only one AP).



### Add user for authentication wifilocal.\*\*.situs

In the upper right click Security and add two guest users with the username and password in lowercase as wel as in uppercase:

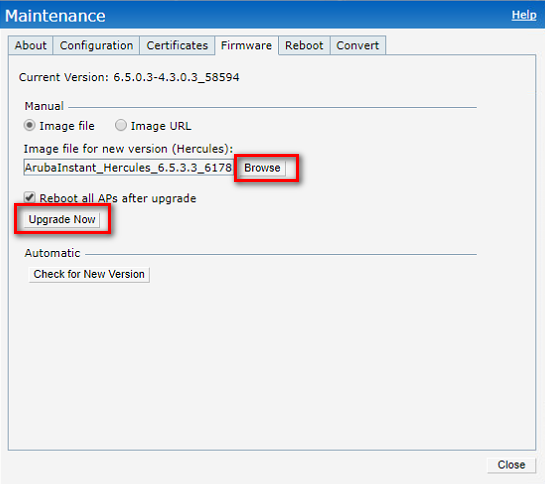
* + Username: <vessel prefix>, example: "ld"
  + Password: <vessel prefix>, example: "ld"

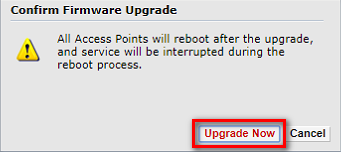


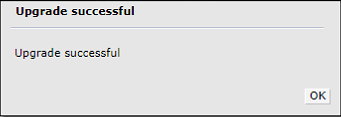
# Firmware update

Firmware location: [\\Jdn-file01\ict\_new\_standard\_sites\_vessels\Firmware\Current](\\\\Jdn-file01\\ict_new_standard_sites_vessels\\Firmware\\Current)

Browse to Firmware and click update now



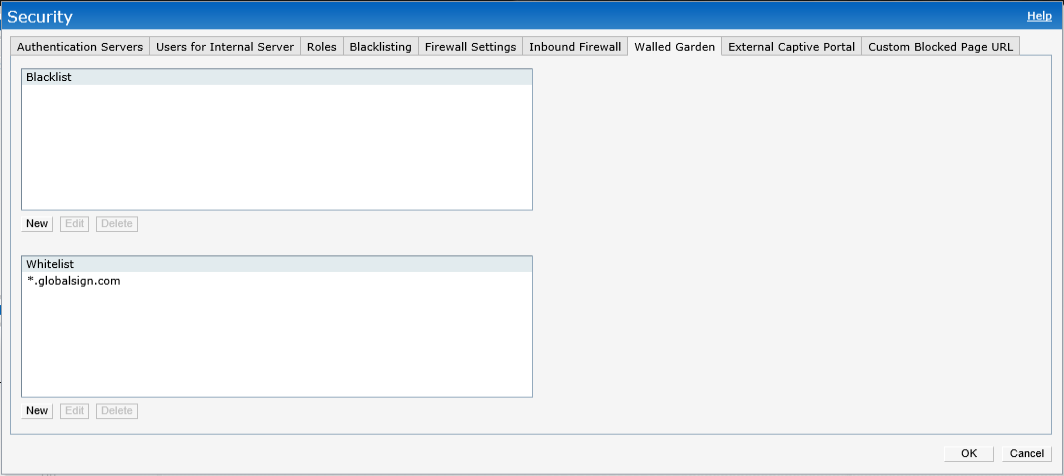




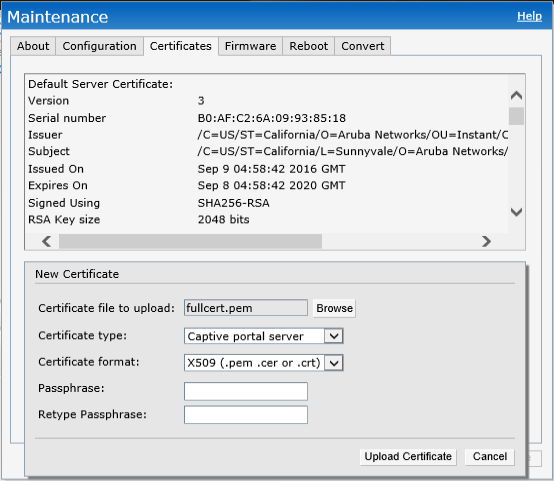
# Certificate update for wifilocal

This is only for ships

1. Go to [\\JDN-FILE01\ict\_new\_standard\_sites\_vessels\Certificate](file:///\\JDN-FILE01\ict_new_standard_sites_vessels\Certificate)
2. Add the vessel to the excel “VesselsWithCert.xlsx”
3. Log in to the Aruba/Dell virtual controller
4. Go to Security -> Walled Garden -> Whitelist -> New -> \*.globalsign.com



1. Go to Maintenance -> Certificates
2. Upload the wifilocal.pem certificate & fill in the password (stored in RDM “Aruba/Dell wifilocal pem password”)



# Configuring individual AP’s

### Zones:

We use zones to restrict broadcasting of SSID’s. Obviously, this is only useful if multiple zones are present, which might not be the case at offices or workshops.

SSID’s tagged with zone "castle" can only be broadcasted by AP’s also tagged with the zone "castle"

SSID’s & AP’s can only be tagged by a single zone.

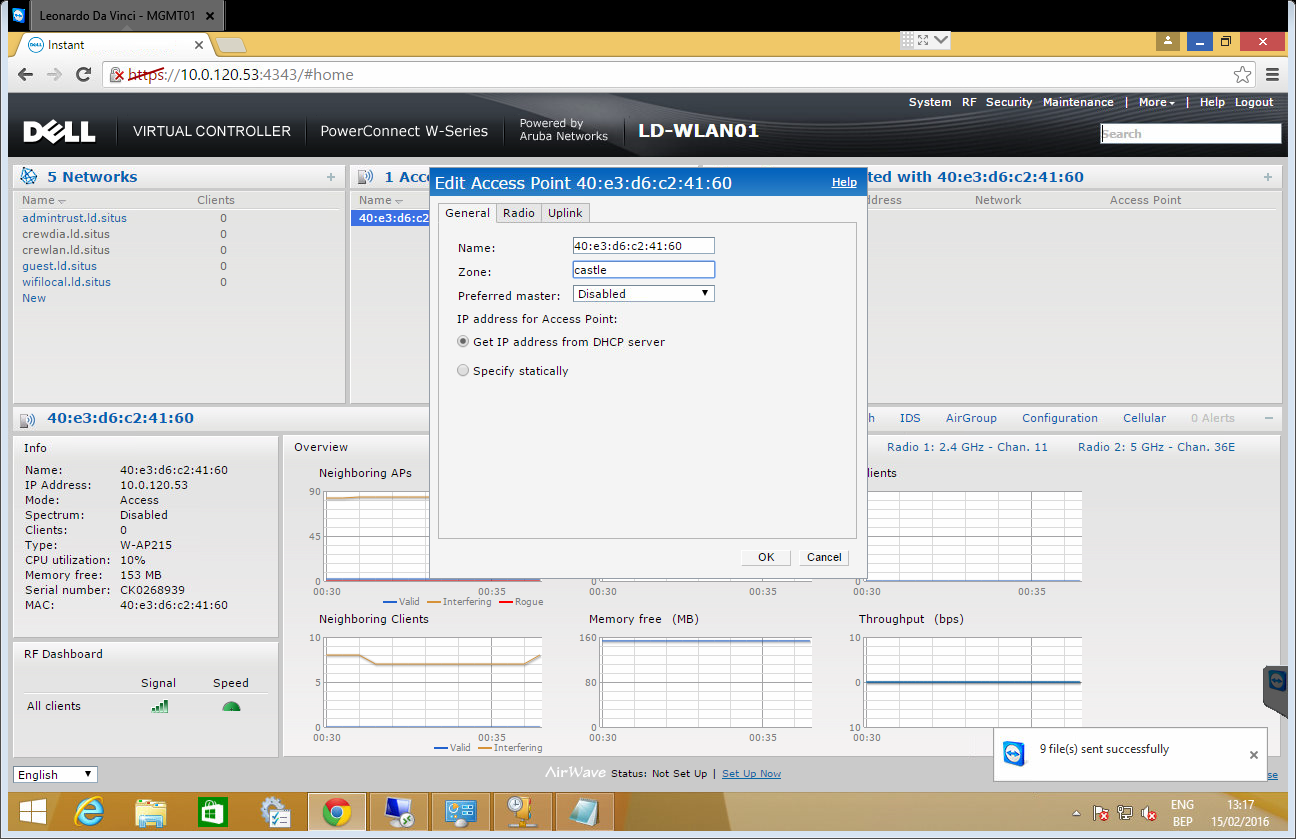
SSID’s without a tag a broadcasted by every AP. (admintrust.\*\*.situs)

### Configuration

Name: give a name to the access point, which defines its location in the vessel.

Example: "B-Deck starboard"

Zone: "castle" if **not** located in a machinery space or store.



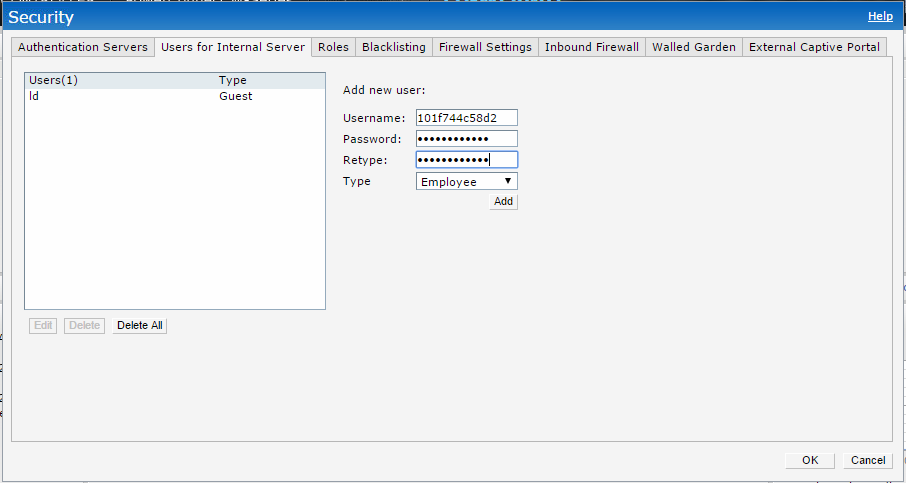
# Whitelisting the MAC address of a barcode scanner

Open "Security" & Click on "Users for Internal Server"

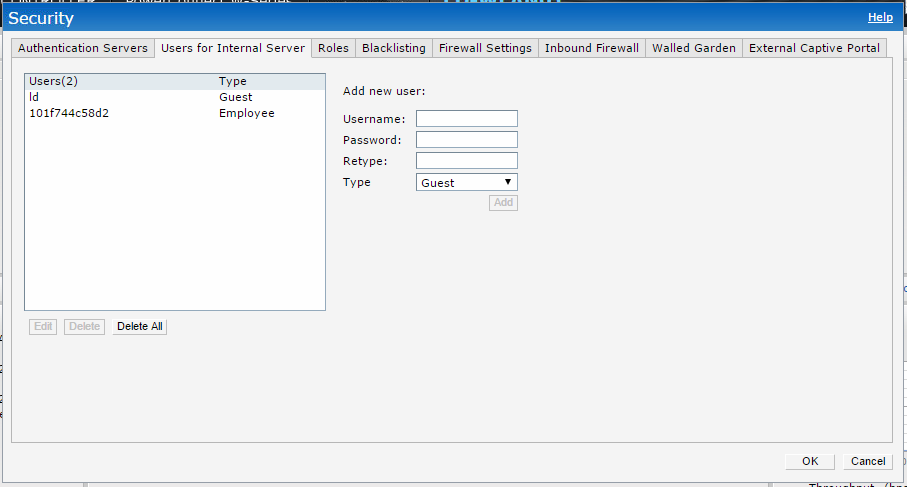
"Add new user:"

* Username: *<mac address>*
* Password: *<mac address>*
* Retype: *<mac address>*
* Type: "Employee"

"Add"



"OK"



# RADIUS - Allowing access to the VPN to JDN devices

At offices and workshops with a VPN connection to JDN Lux & Be, it is possible to set up a network with RADIUS authentication to allow restricted access:

Requirements for utilizing these networks:

* Add user to: JDN\_GSR\_WIFI\_ACCESS\_ON\_ALL\_SITES\_USERS

cid:image011.jpg@01D17569.5B773550

* Manually configure the wifi connection on the user’s computer, using:
  + WPA2-Enterprise
  + AES
  + Under network authentication method, press Settings & disable server certificate validation and enable automatic use of windows login and password.

