|  |
| --- |
| **JDN Standards – Dell IAP** |

Introduction 2

Available WiFi networks 3

Switch setup 5

Preparation 5

Configuration 5

Virtual controller setup 6

Preparation 6

Configuration 6

SSID creation 10

Vessels 10

admintrust.\*\*.situs 10

crewdia.\*\*.situs 12

crewlan.\*\*.situs 15

guest.\*\*.situs 18

leisure.\*\*.situs 21

wifilocal.\*\*.situs 21

Sites 24

admintrust.\*\*.situs 24

adminuntrustdata.\*\*.situs 26

adminuntrustvoice.\*\*.situs 29

guest.\*\*.situs 31

JDN integrated sites 33

REMOTE\_RF\_DATA 33

XXX\_GUEST 37

Configuring individual AP’s 39

Zones: 39

Configuration 39

Whitelisting the MAC address of a barcode scanner 40

RADIUS - Allowing access to the VPN to JDN devices 41

# Introduction

This document describes the technical wifi setup of the standards as defined for JDN deployments in 2015. 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 905
  + **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

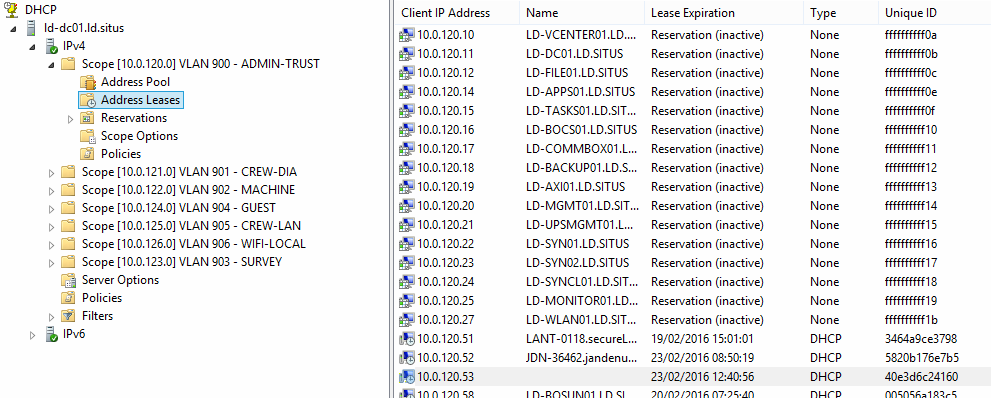
**Warning:** Never manually add "*unit 0 family ethernet-switching vlan members* ***admin-trust***" to the VLAN trunk presented to the access points! Since admin-trust (vlan 900) is already the native-vlan, it does not need to be added separately. Doing so will cause packet drops an eratic behavior.

# Virtual controller setup

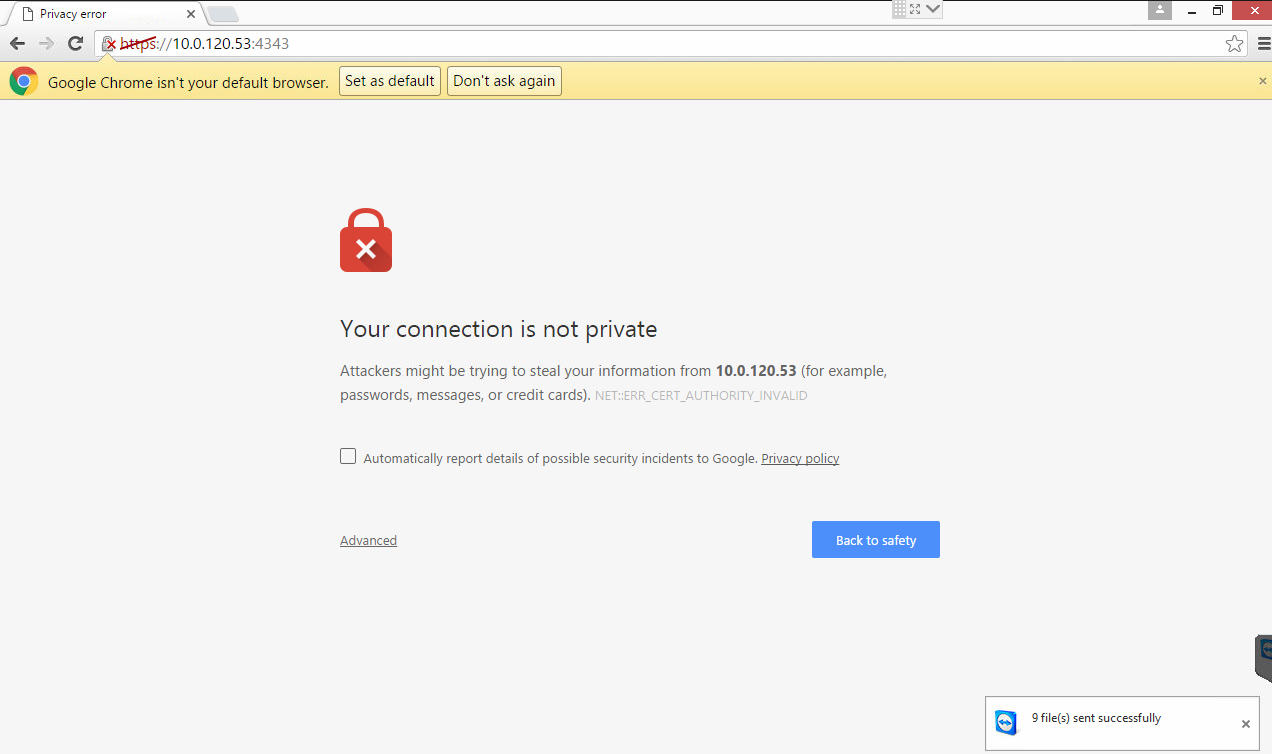
## Preparation

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.

## Configuration

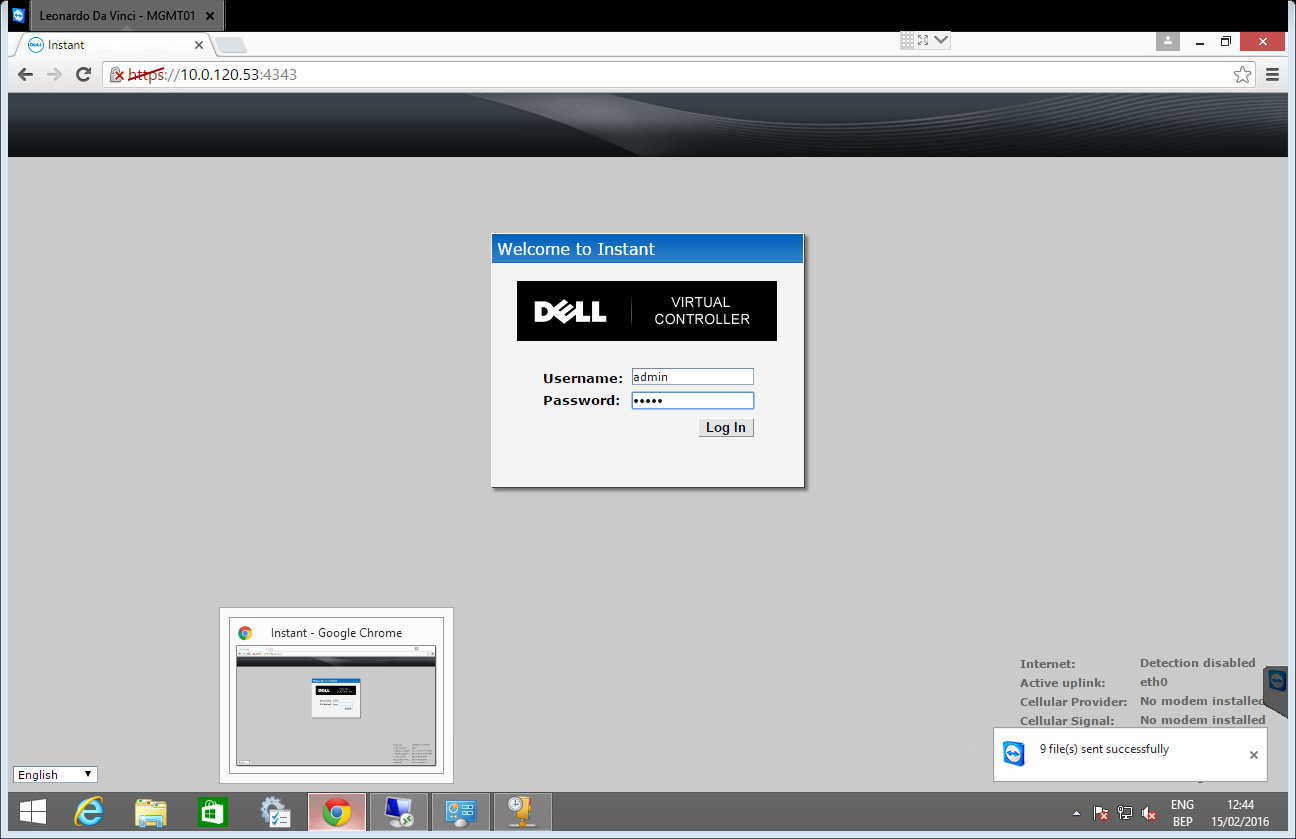
When the AP is booted, you will notice it will start broadcasting an "instant" SSID. You will also find a DHCP lease in the ADMIN-TRUST DHCP scope. You can double check with its mac address.

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

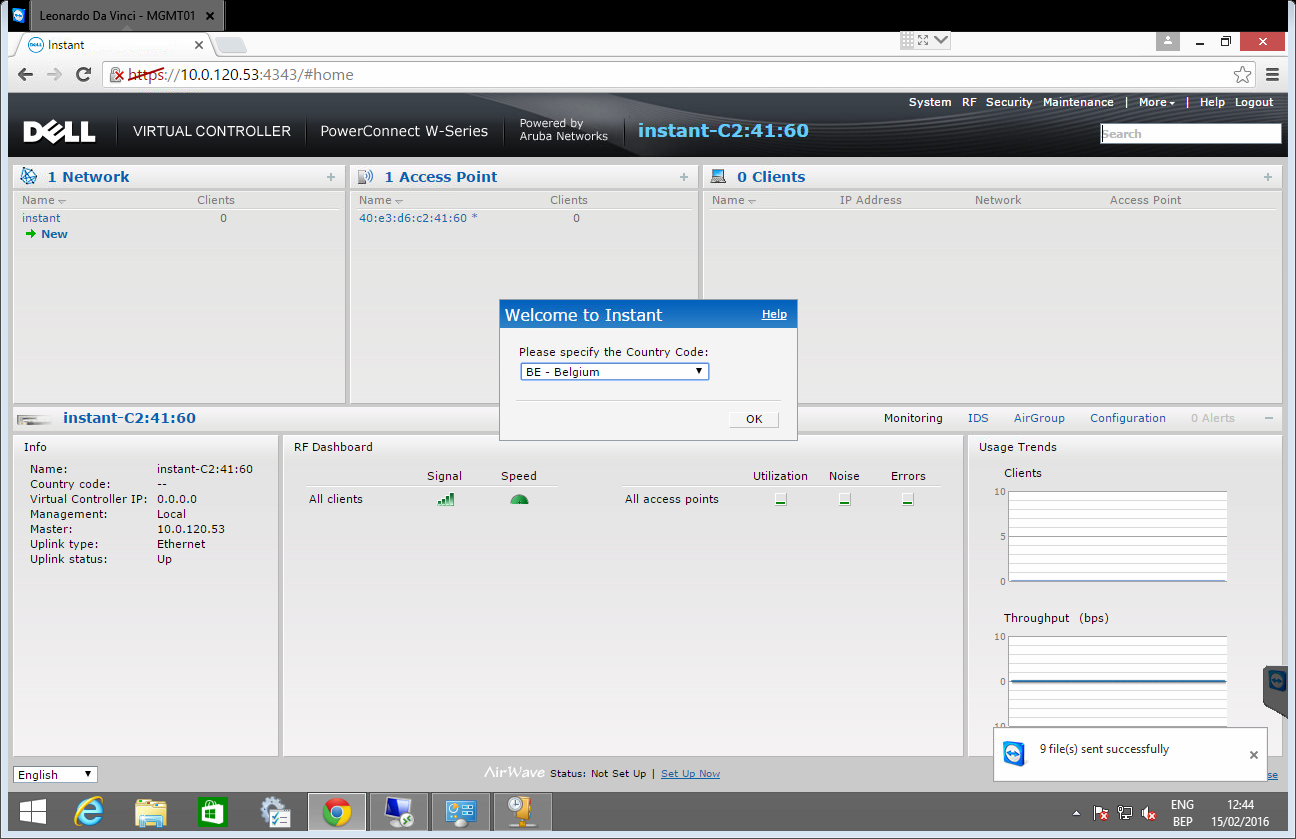


Login with the following default credentials

* Username: admin
* Password: admin



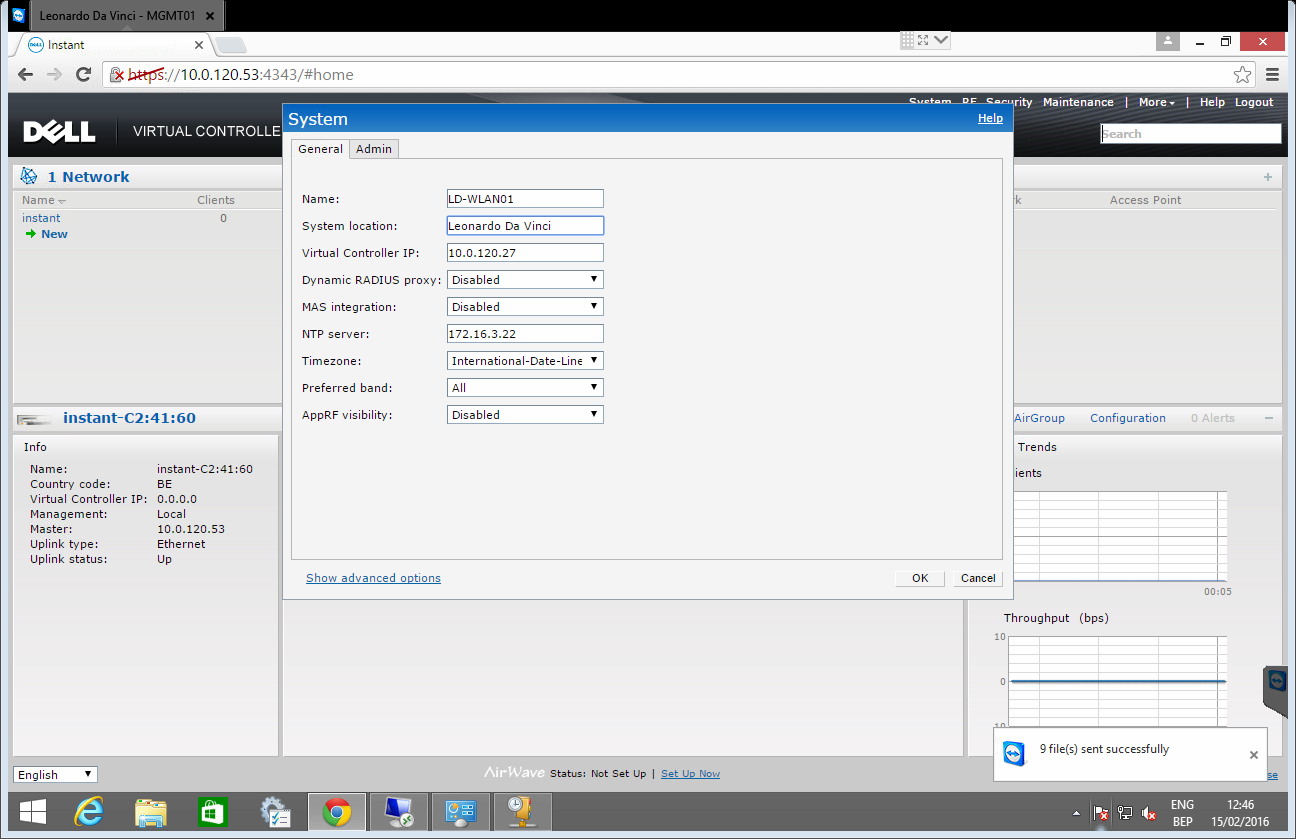
Select "BE – Belgium" as country code.



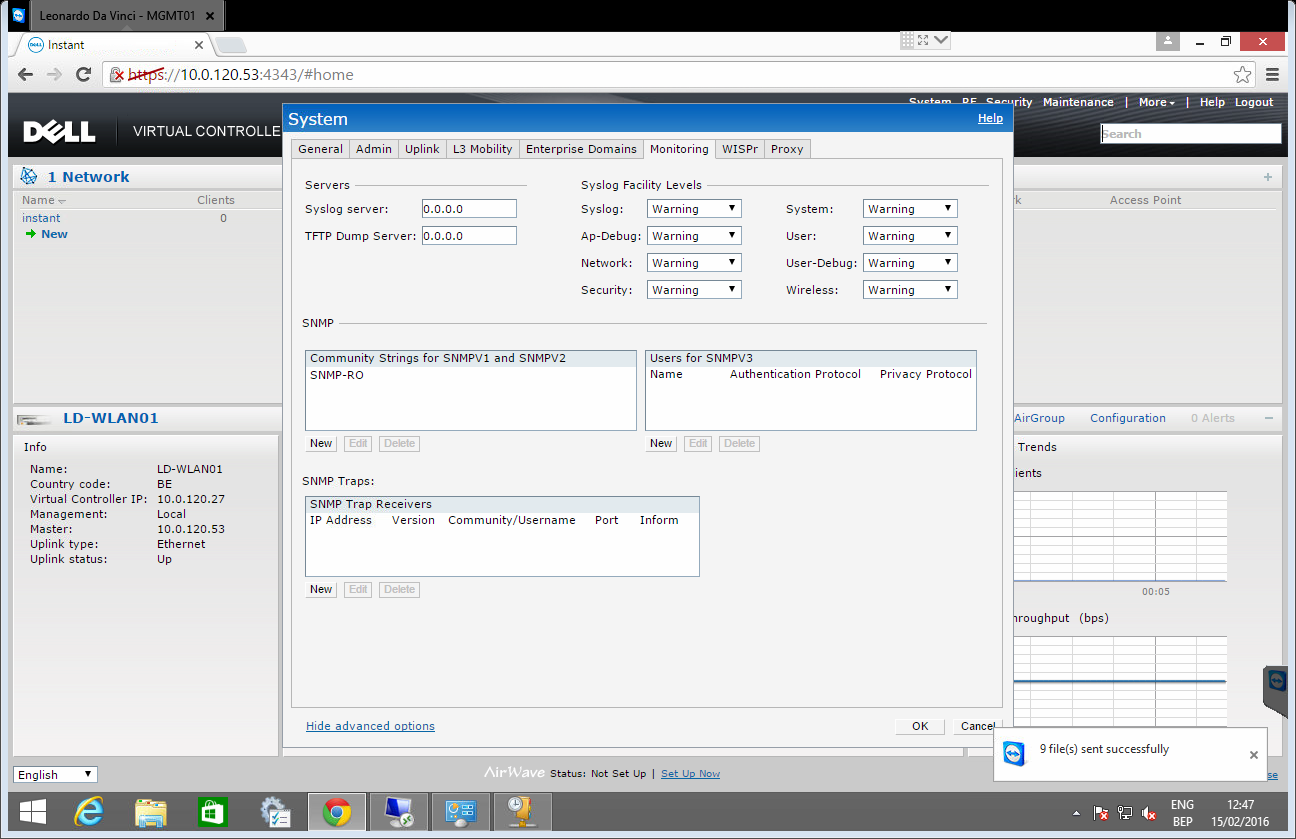
Go to "System", and change the following values:

* Name: \*\*-WLAN01
* System location: <vessel/office name>
* Virtual controller IP: 10.\*\*\*.\*\*\*.27
* NTP server: 172.16.3.22

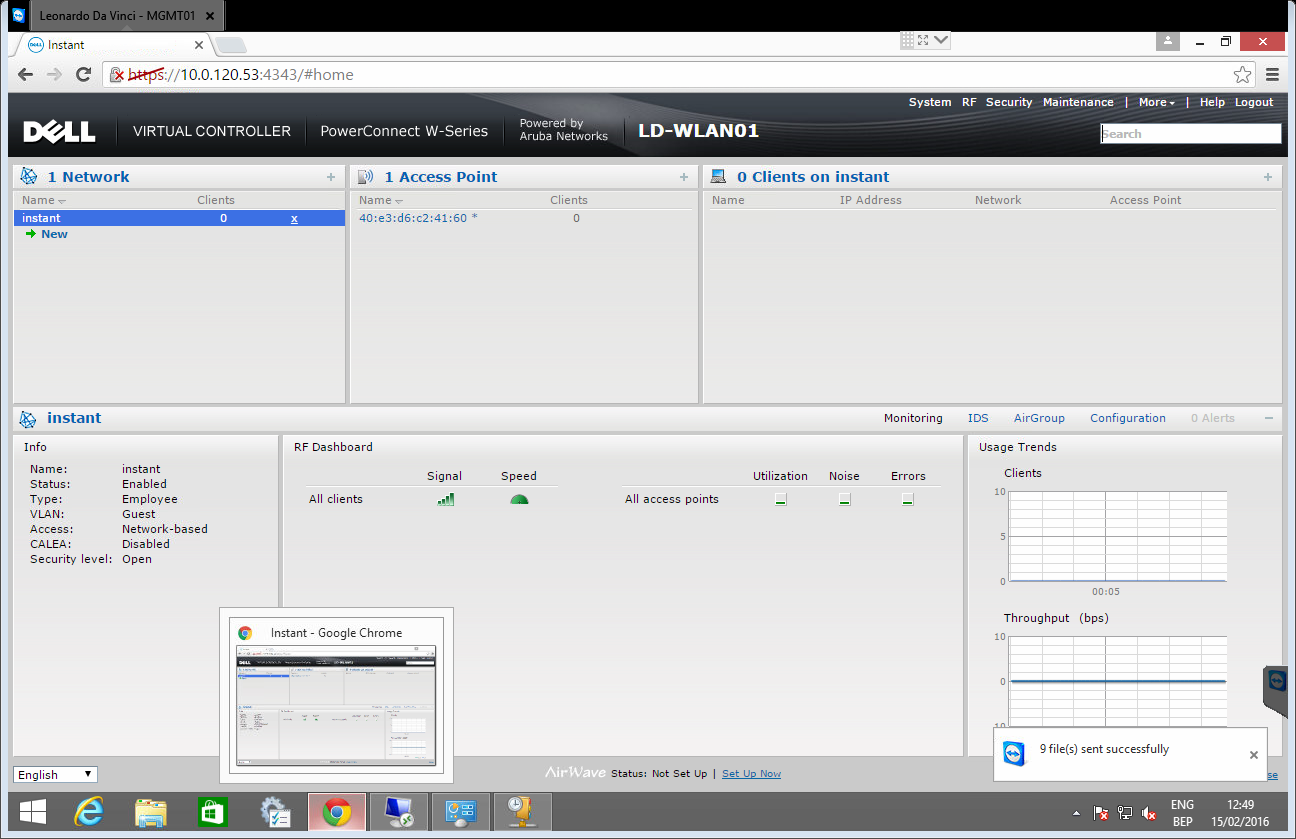
Also change the admin password on the "Admin" tab.



Click "Show advanced options", open the "Monitoring" tab and add the "SNMP-RO" community string.



Delete SSID "instant"



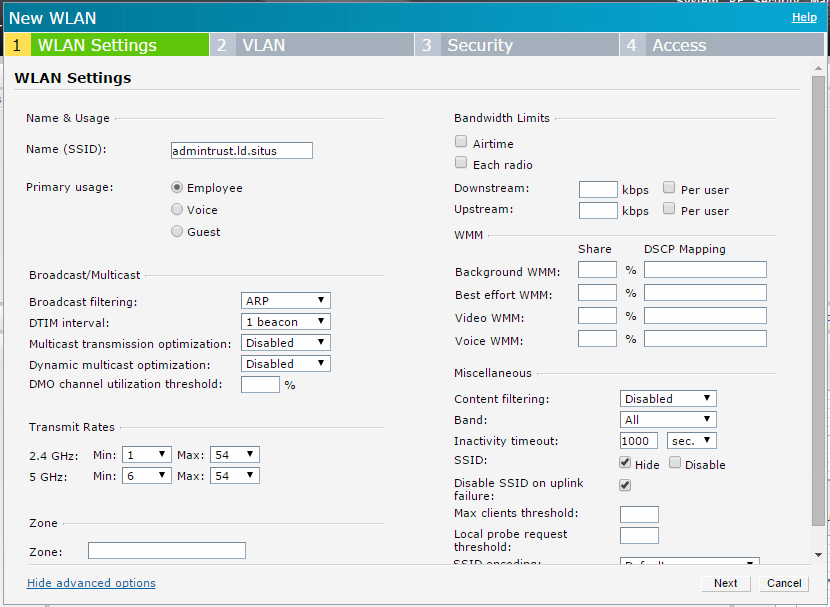
# SSID creation

## Vessels

### admintrust.\*\*.situs

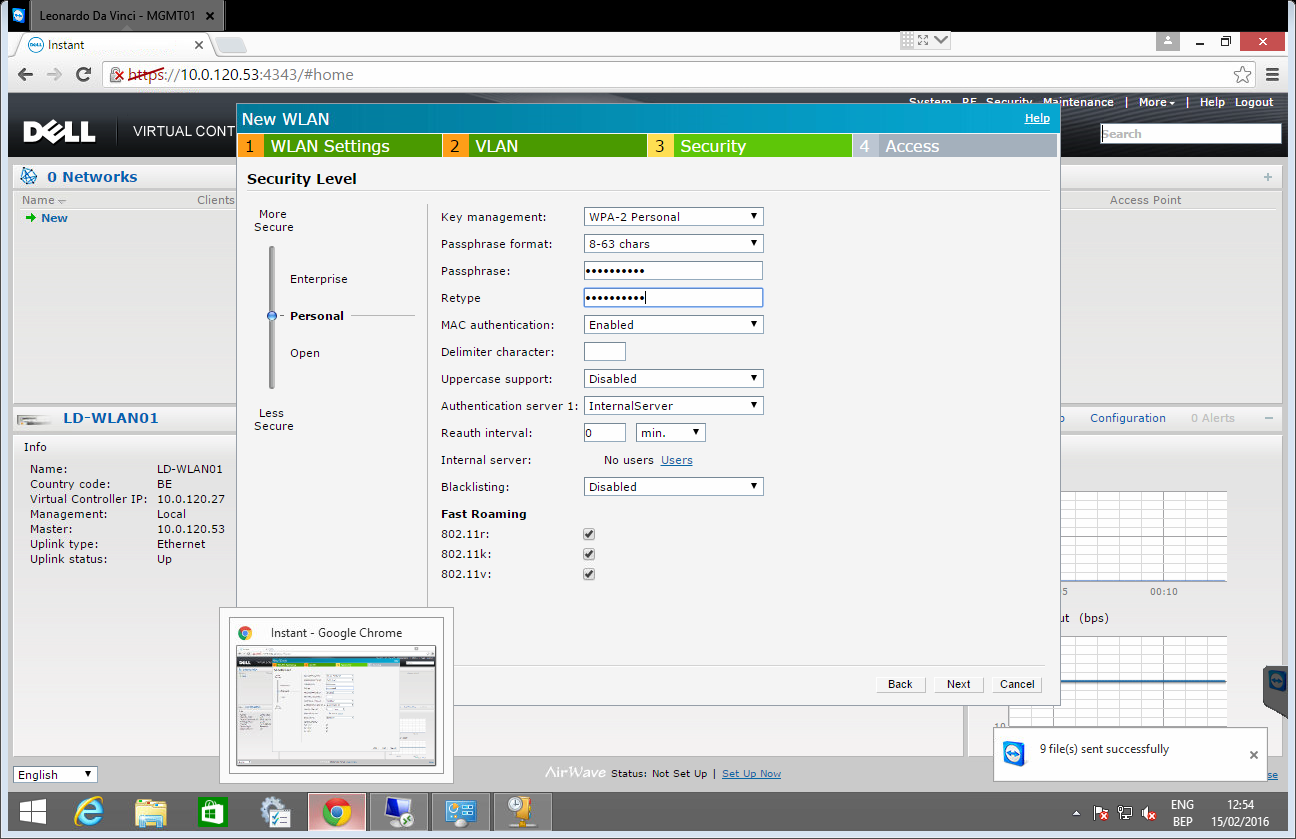
Click on "new" and "Show advanced options"

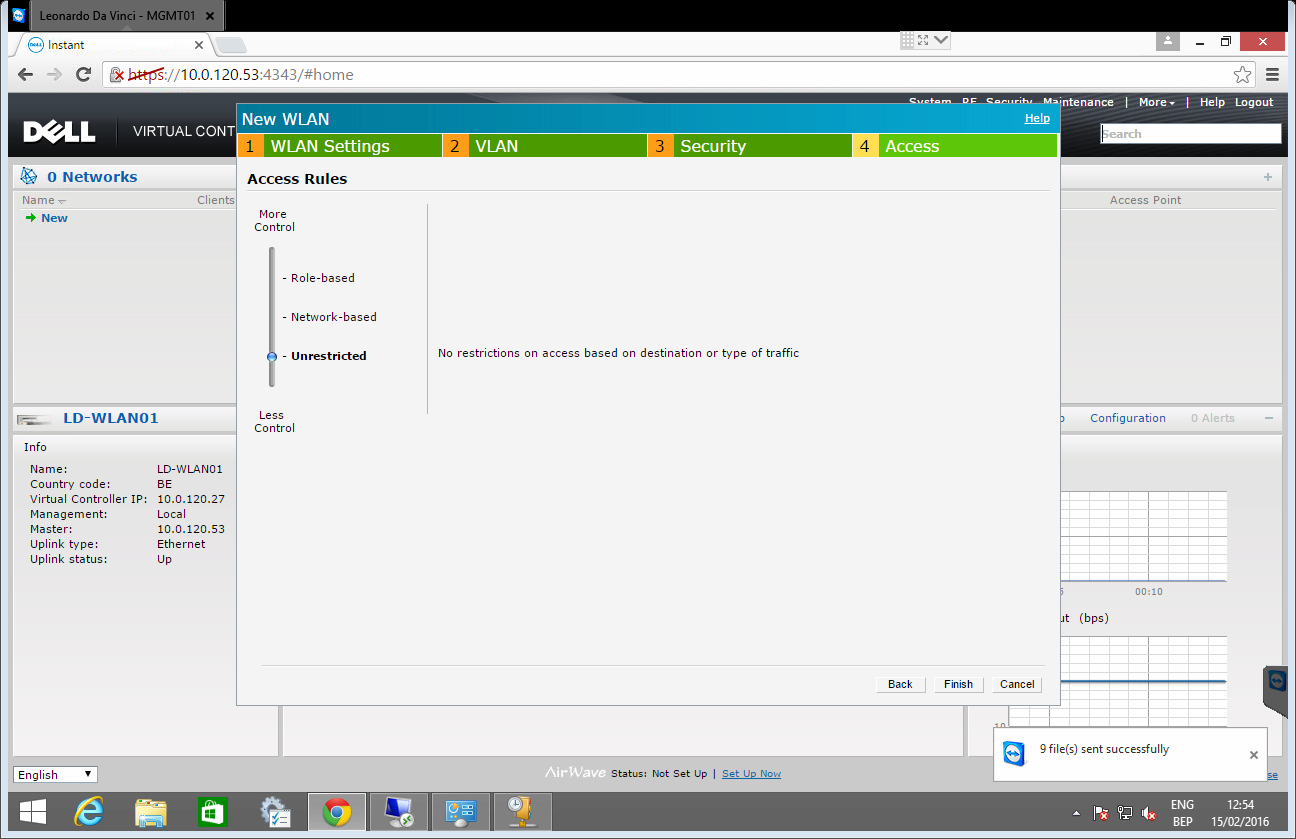
* Name (SSID): admintrust.\*\*.situs
* SSID: Hide



"Next" and change the values below:

* WPA-2 Personal
* Mac authentication: "Enabled"
* Fast roaming: on

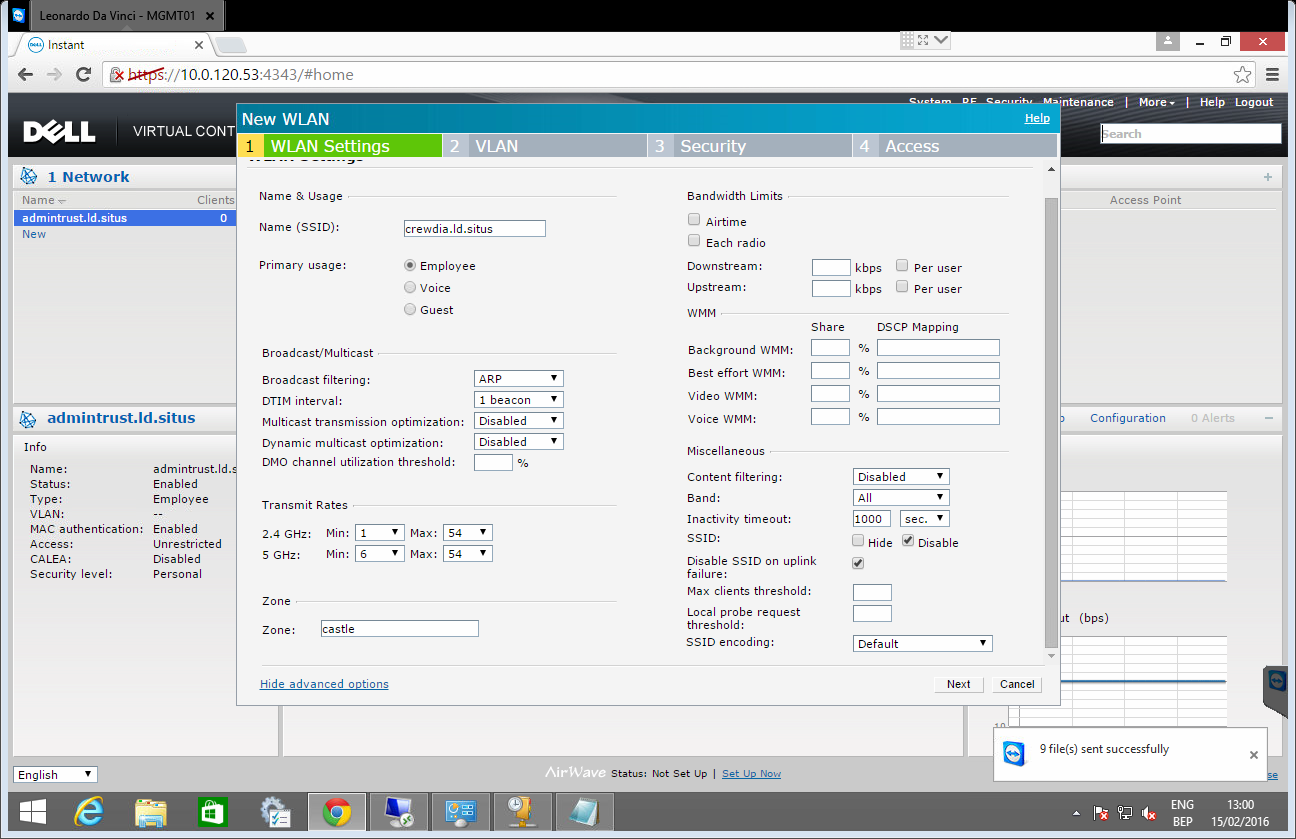




### crewdia.\*\*.situs

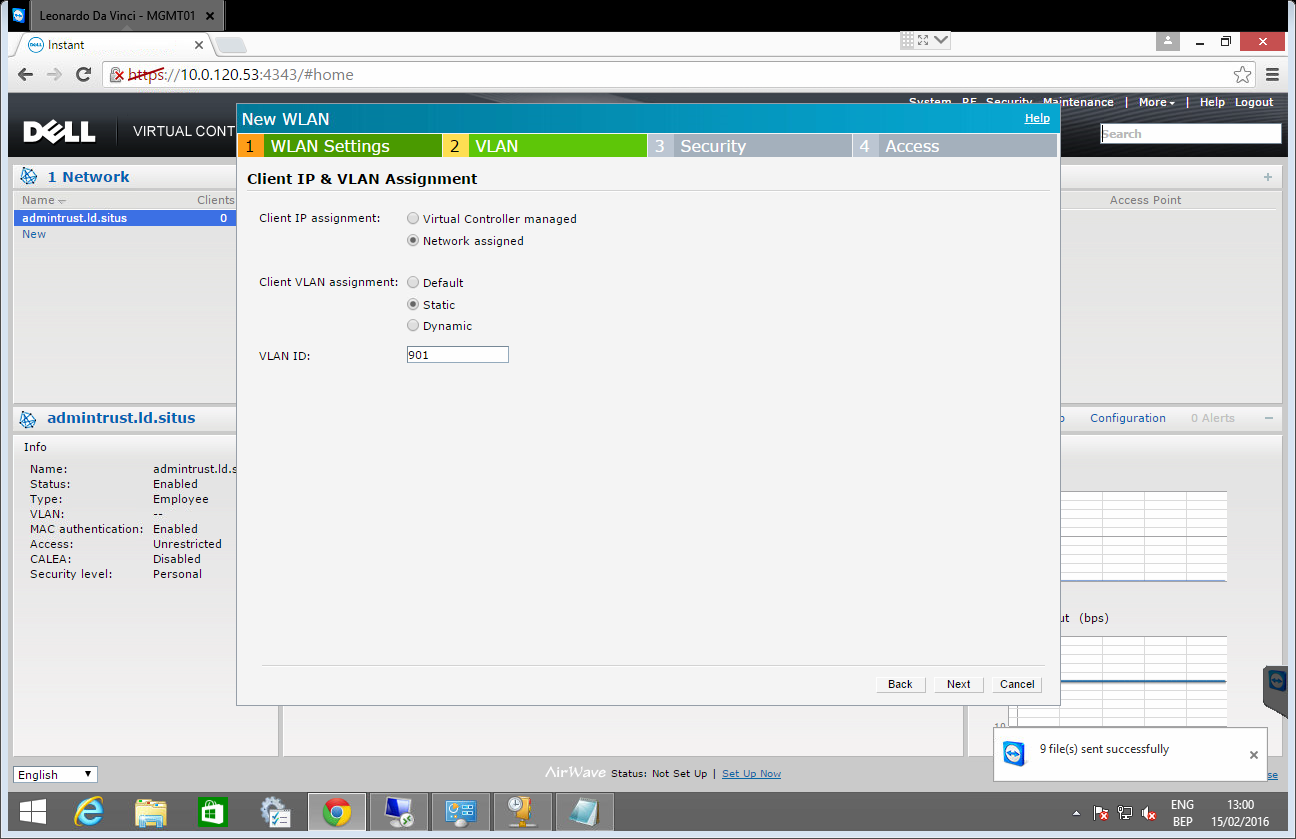
Click on "new" and "Show advanced options"

* Name (SSID): crewdia.\*\*.situs
* SSID: Disable
* Zone: castle



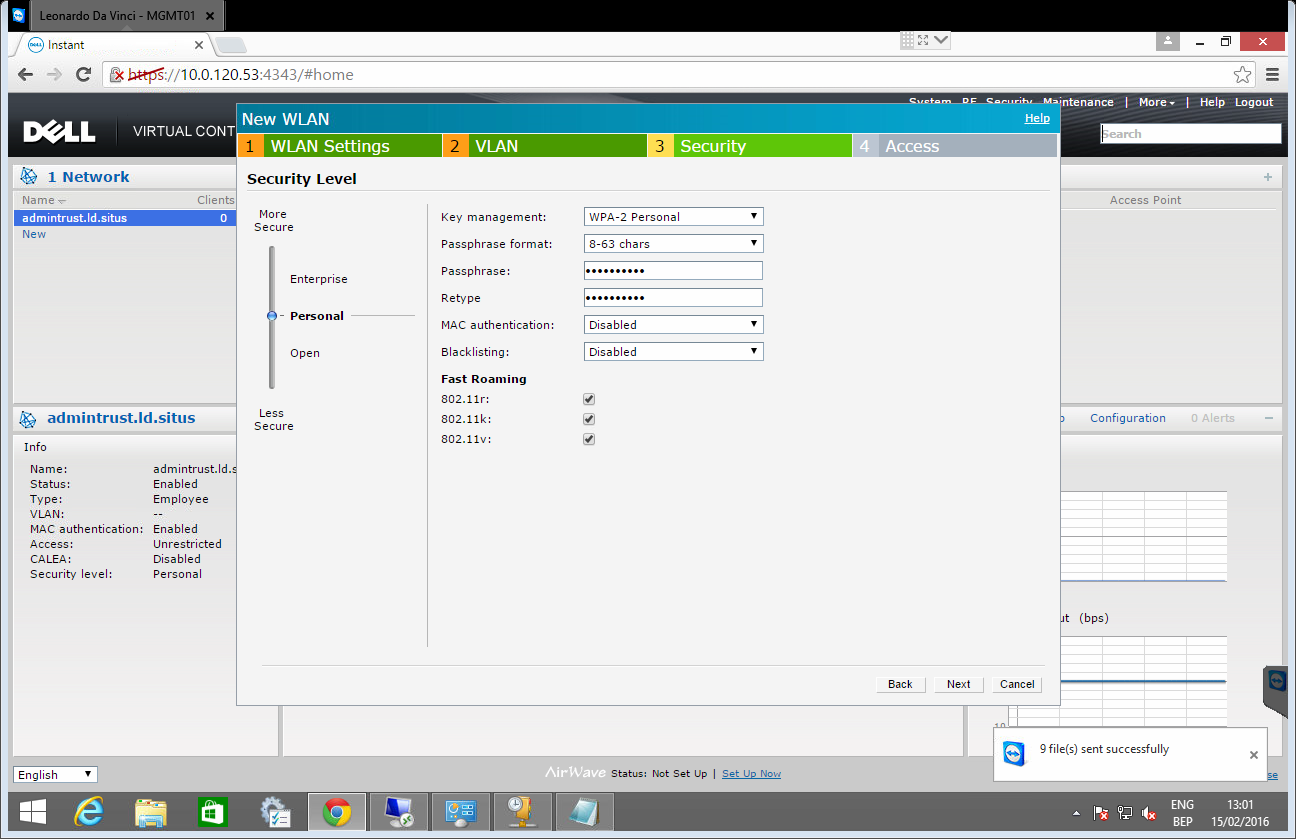
"Next"

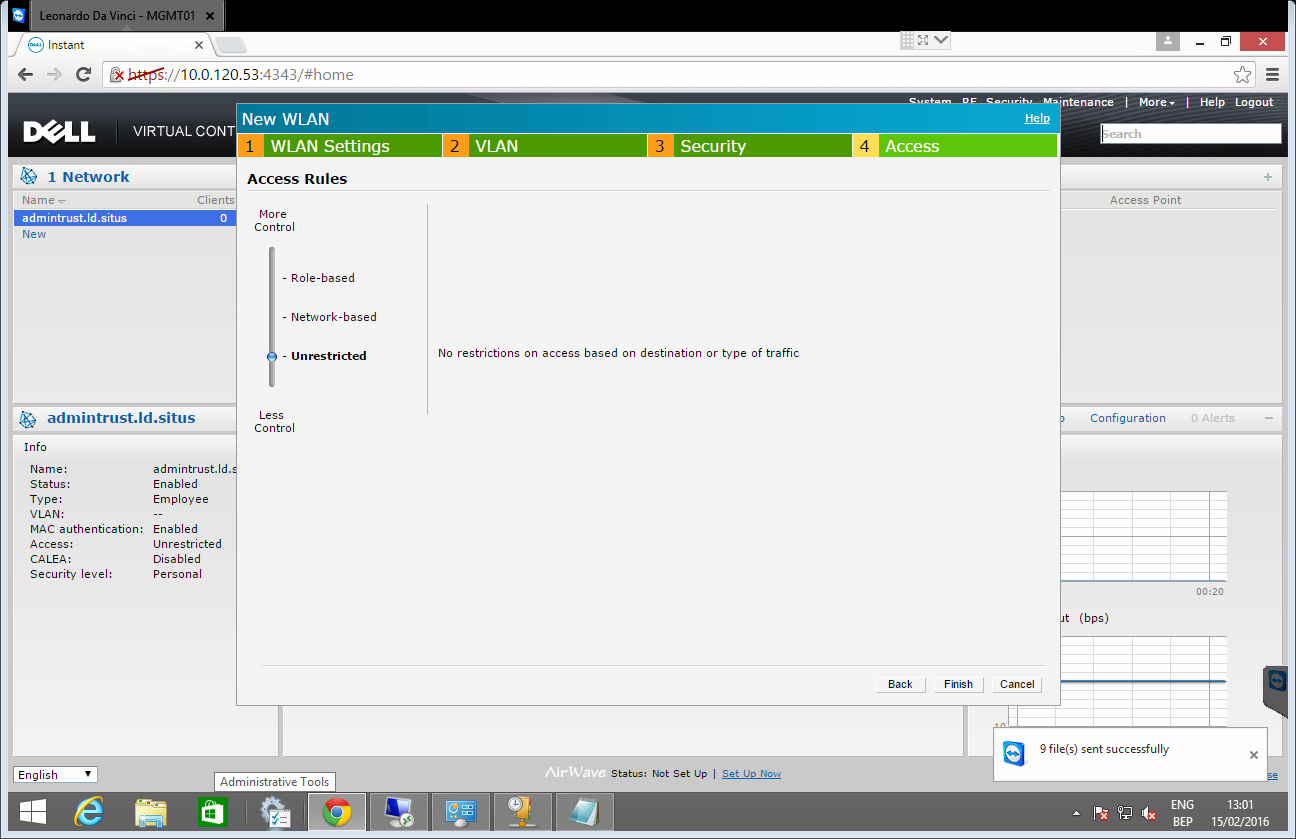
* Client VLAN assignment: Static
* VLAN ID: 901



"Next"

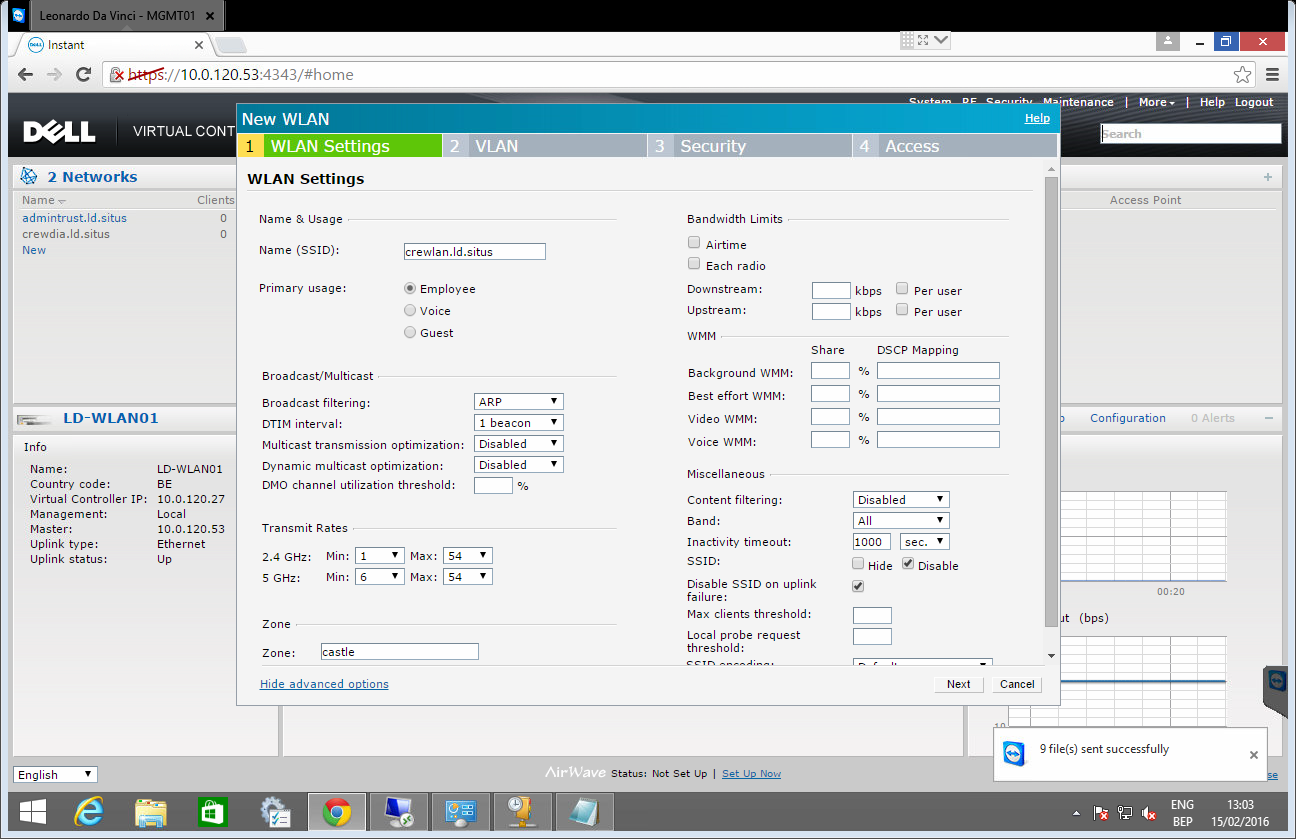
* WPA-2 Personal
* Fast roaming: on





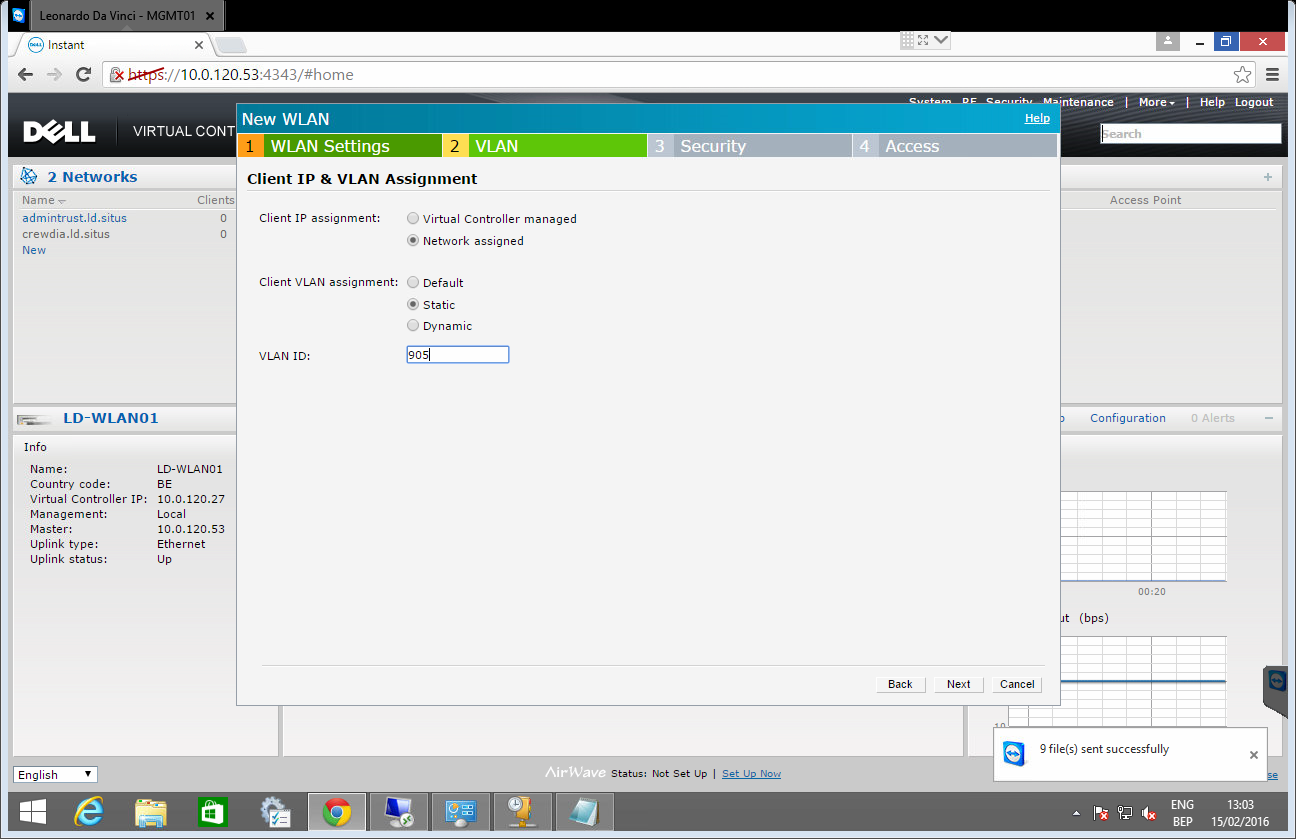
### crewlan.\*\*.situs

* Name (SSID): crewlan.\*\*.situs
* Zone: castle
* SSID: Disable



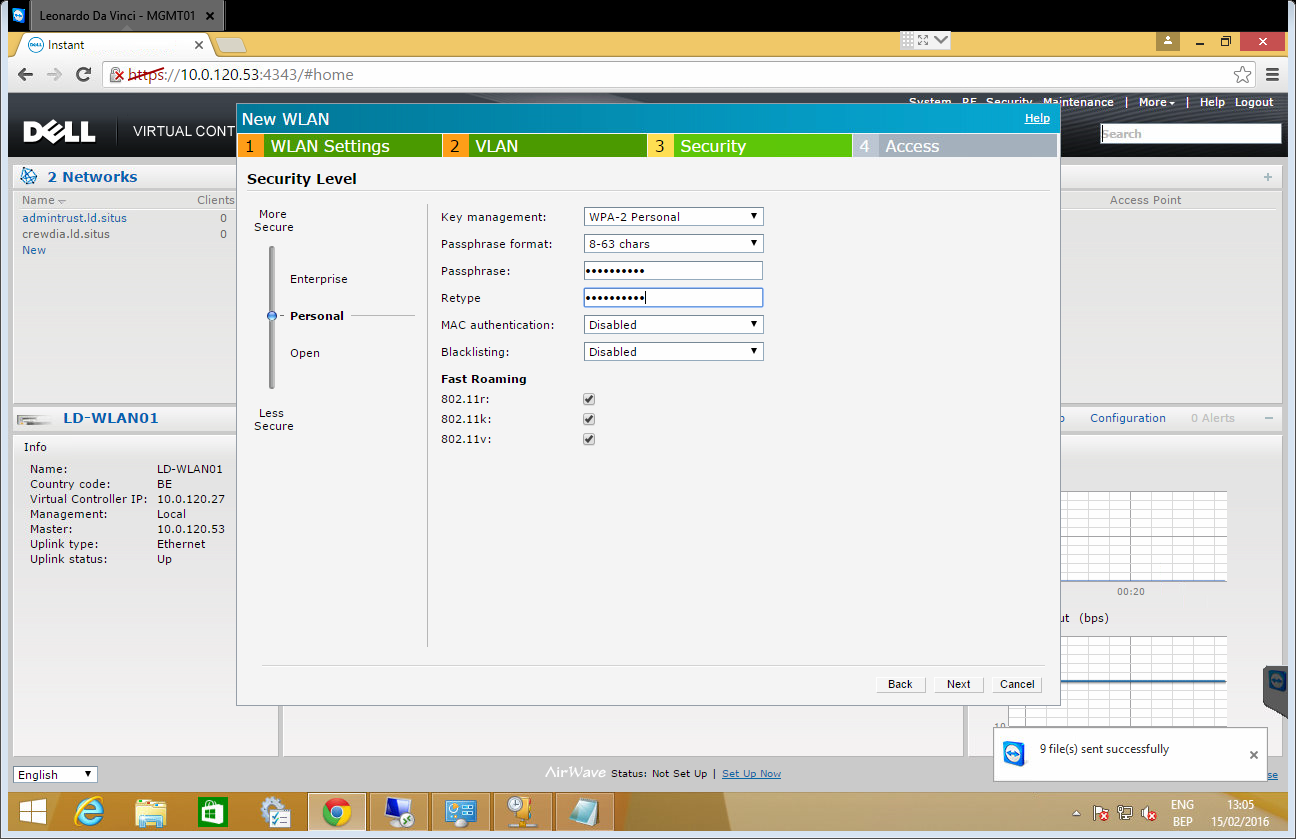
"Next"

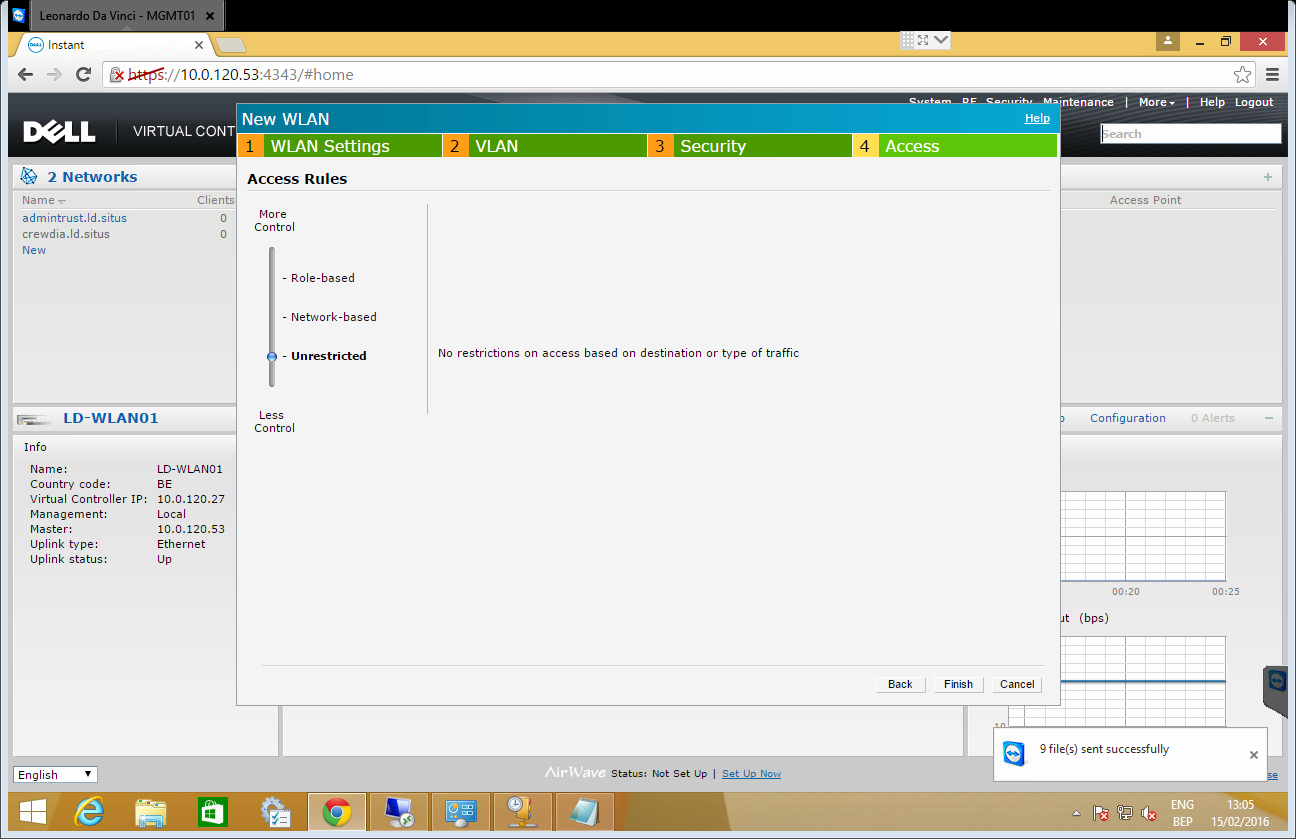
* Client VLAN assignment: Static
* VLAN ID: 905



"Next"

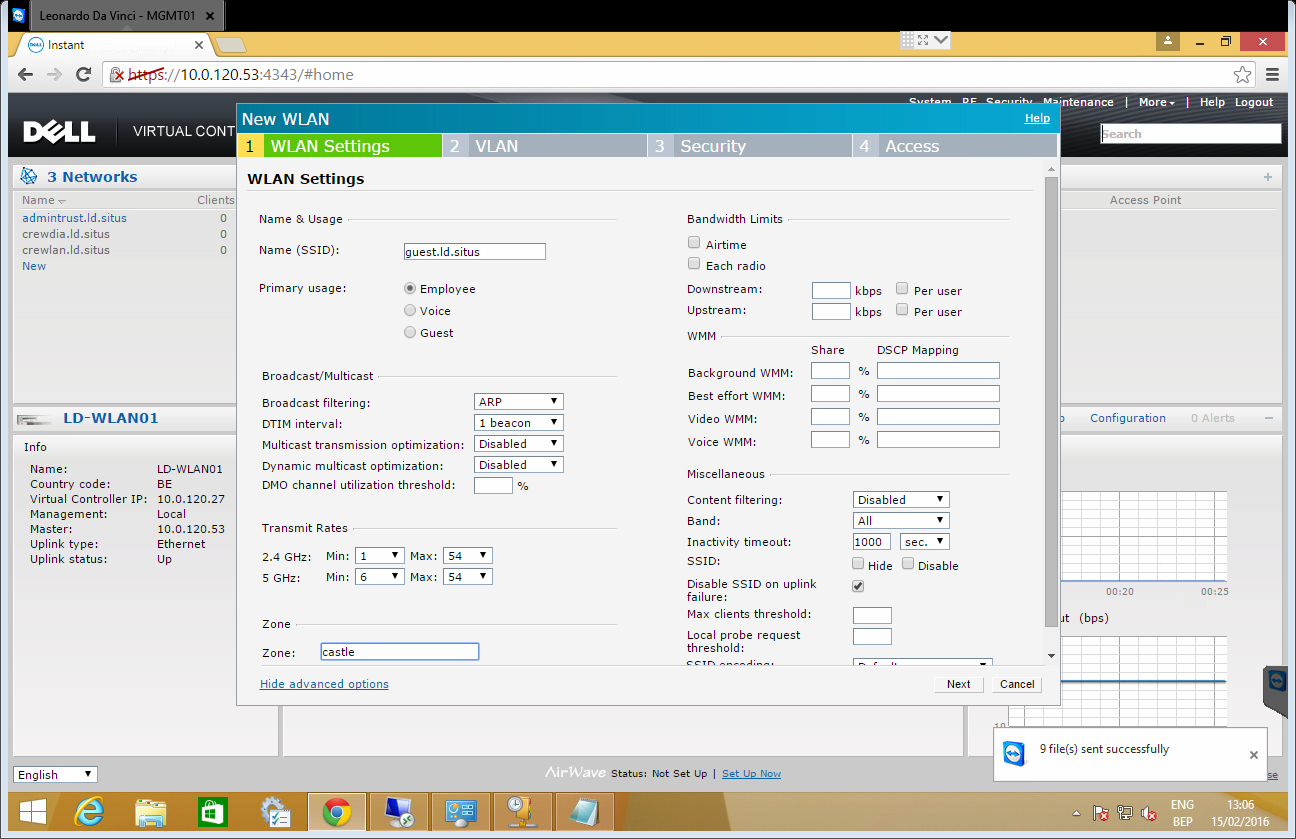
* WPA-2 Personal
* Fast roaming: on





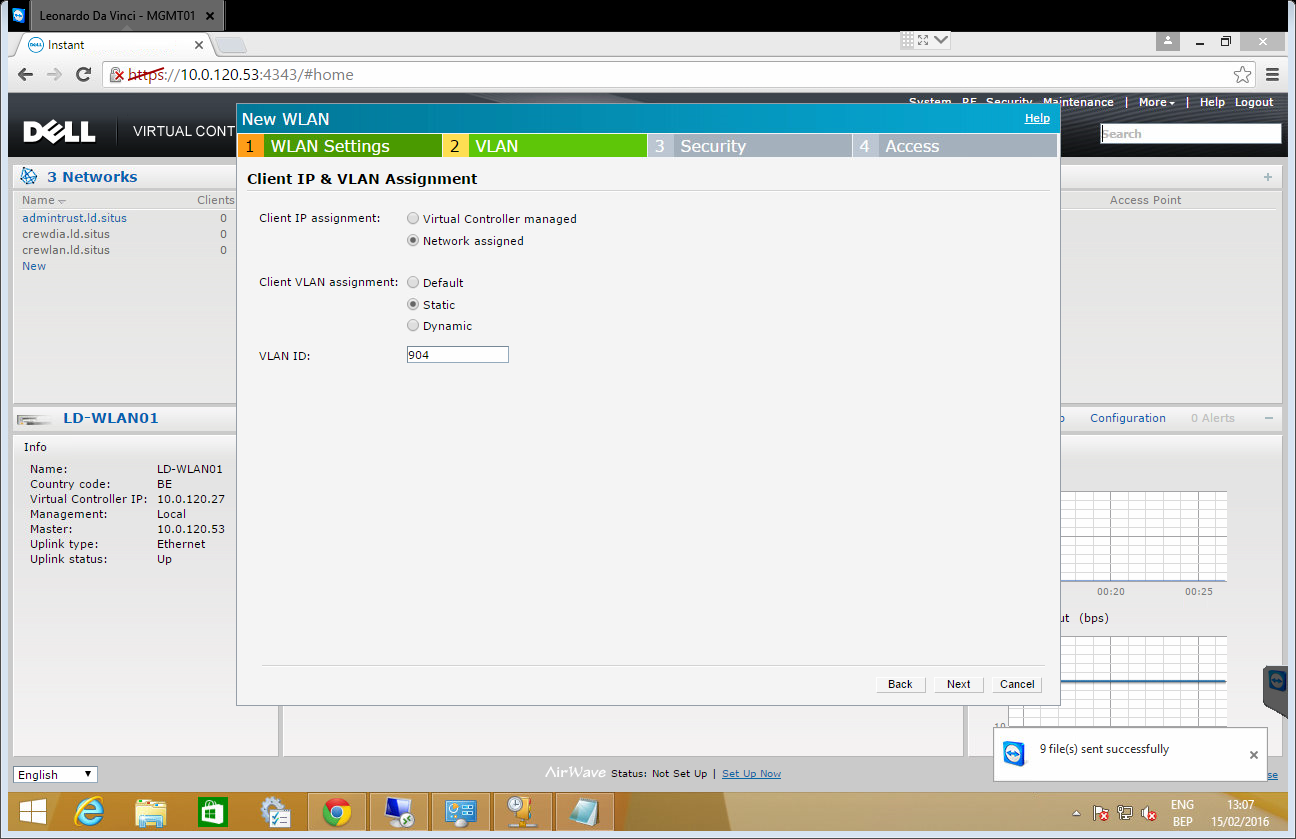
### guest.\*\*.situs

* Name SSID: guest.\*\*.situs
* Zone: castle



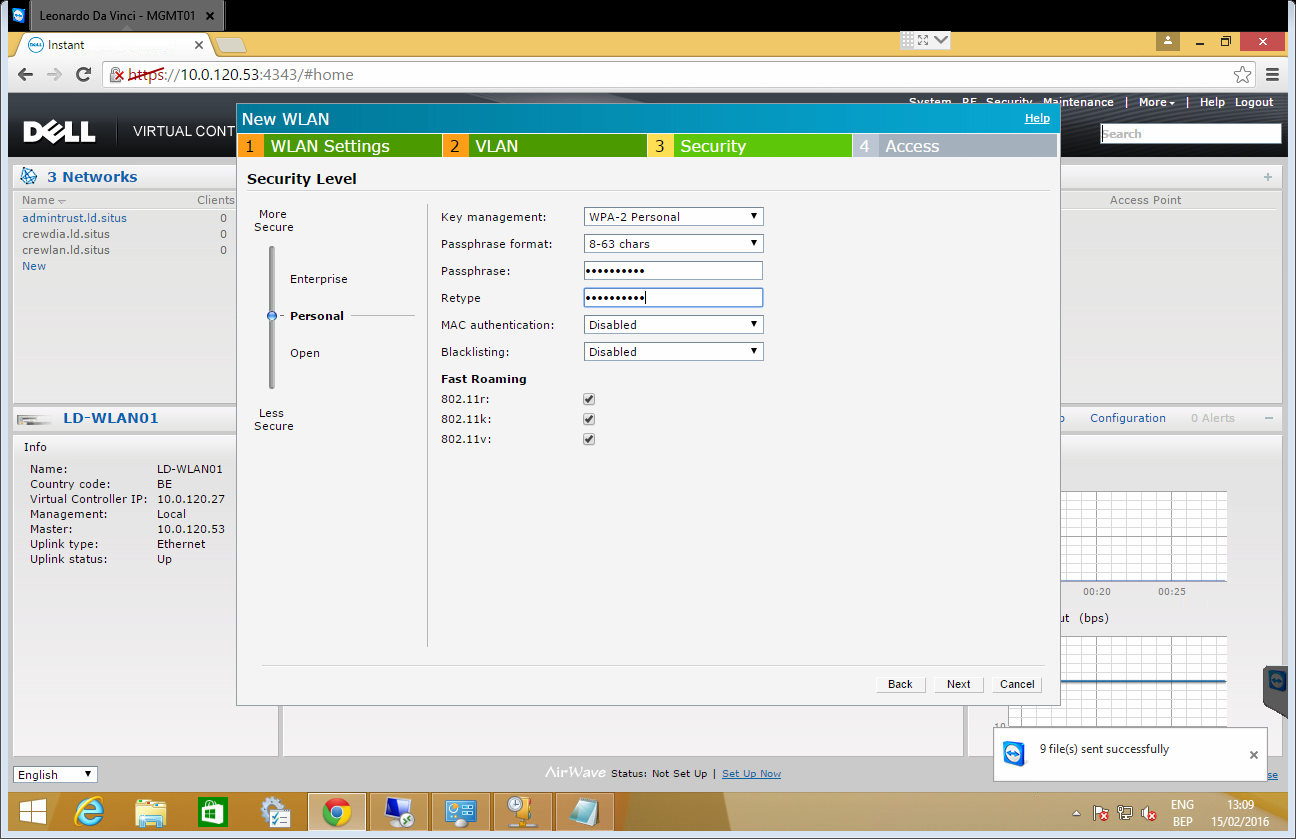
"Next"

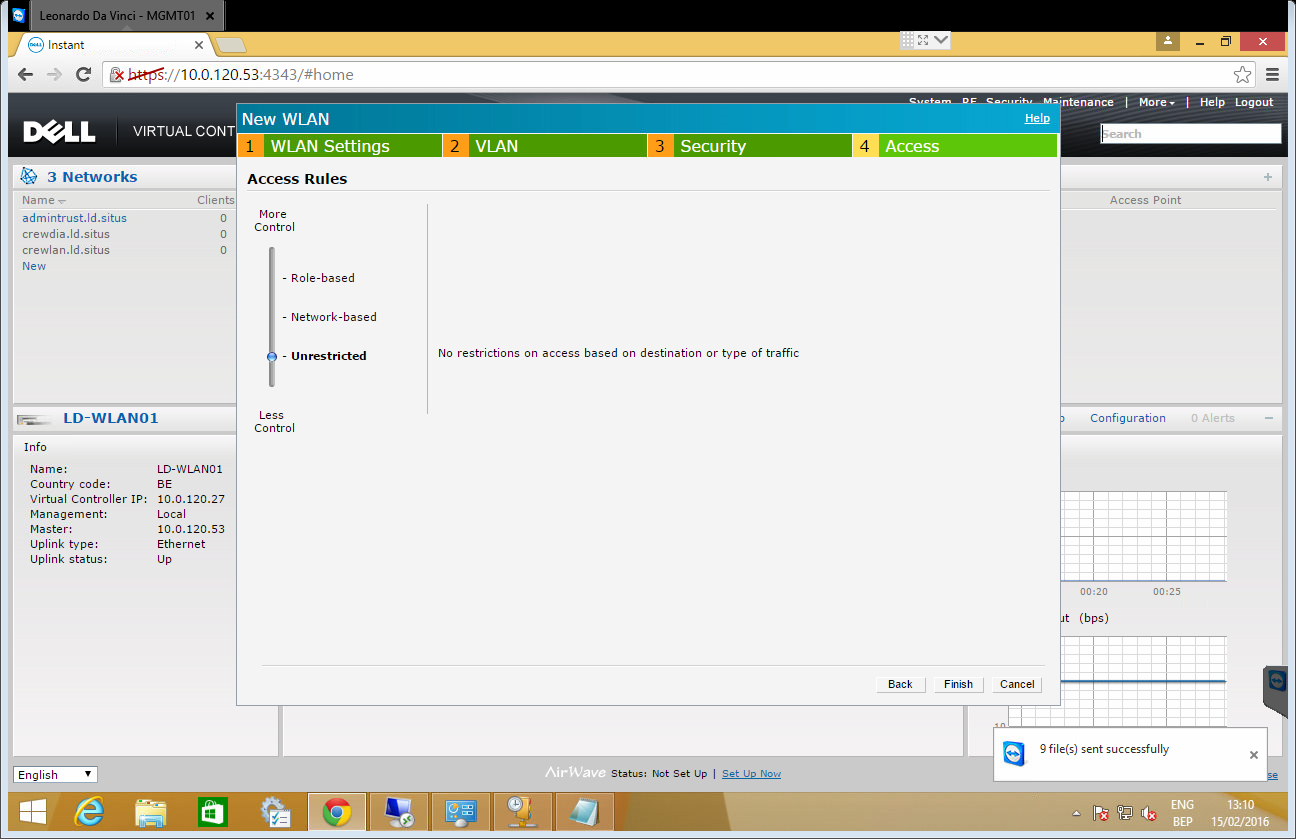
* Client VLAN assignment: Static
* VLAN ID: 904



"Next"

* WPA-2 Personal
* Fast roaming: on



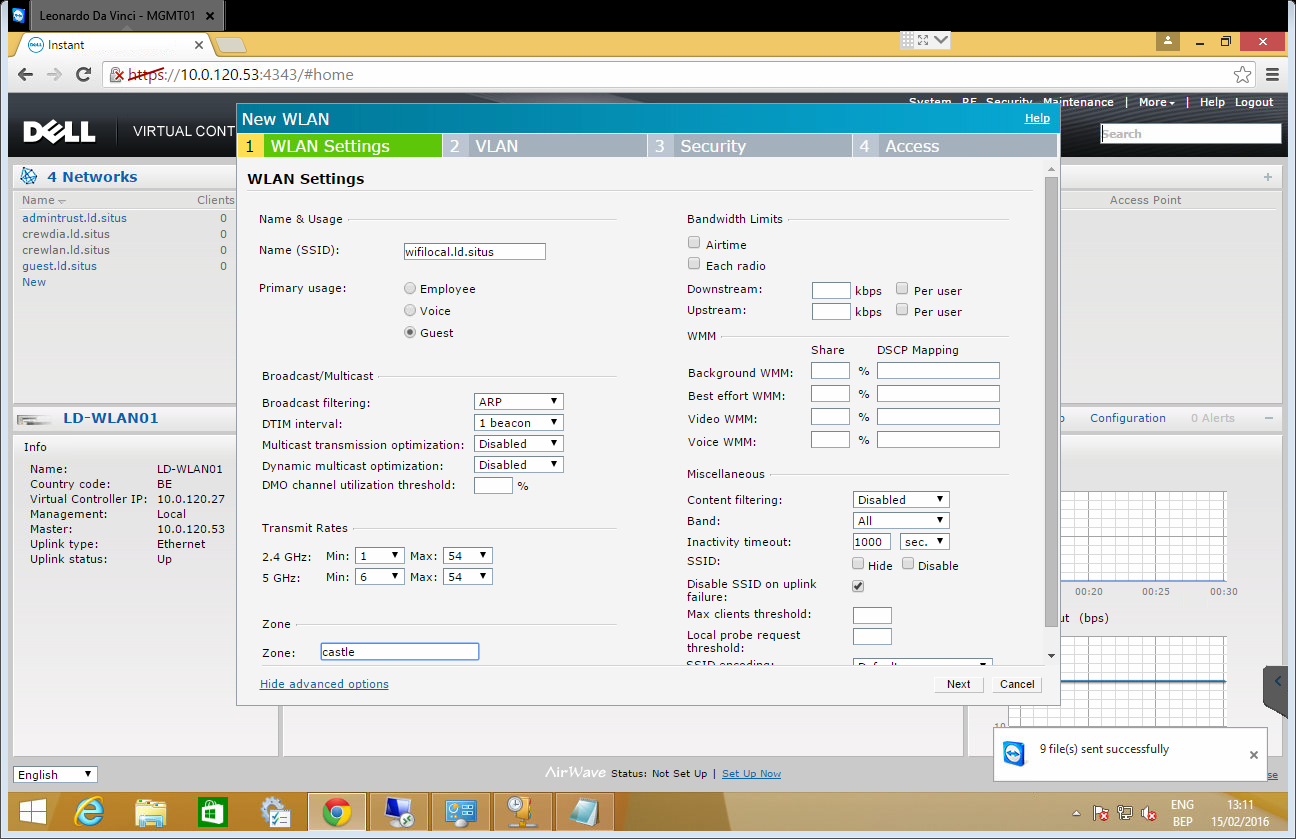


### leisure.\*\*.situs

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

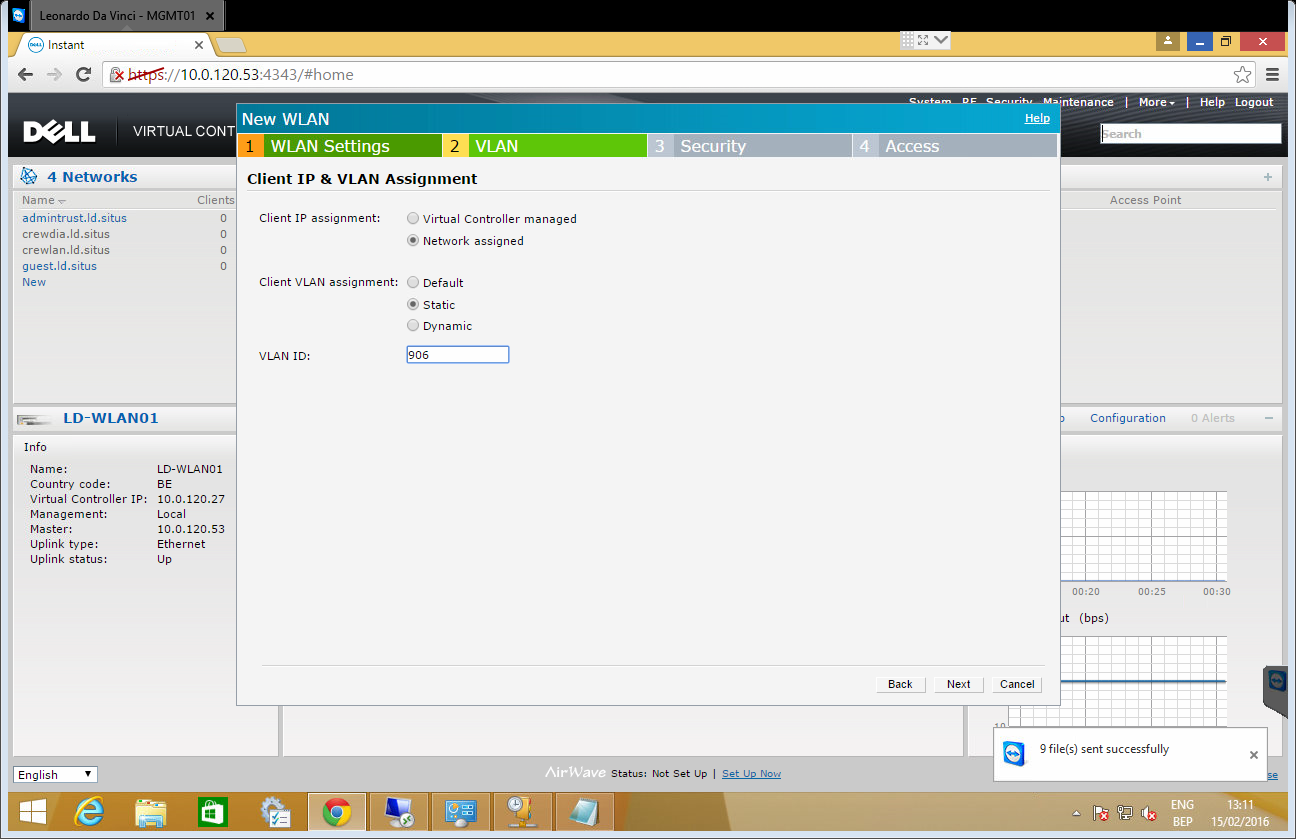
### wifilocal.\*\*.situs

* Name SSID: wifilocal.\*\*.situs
* Primary usage: guest
* Zone: castle



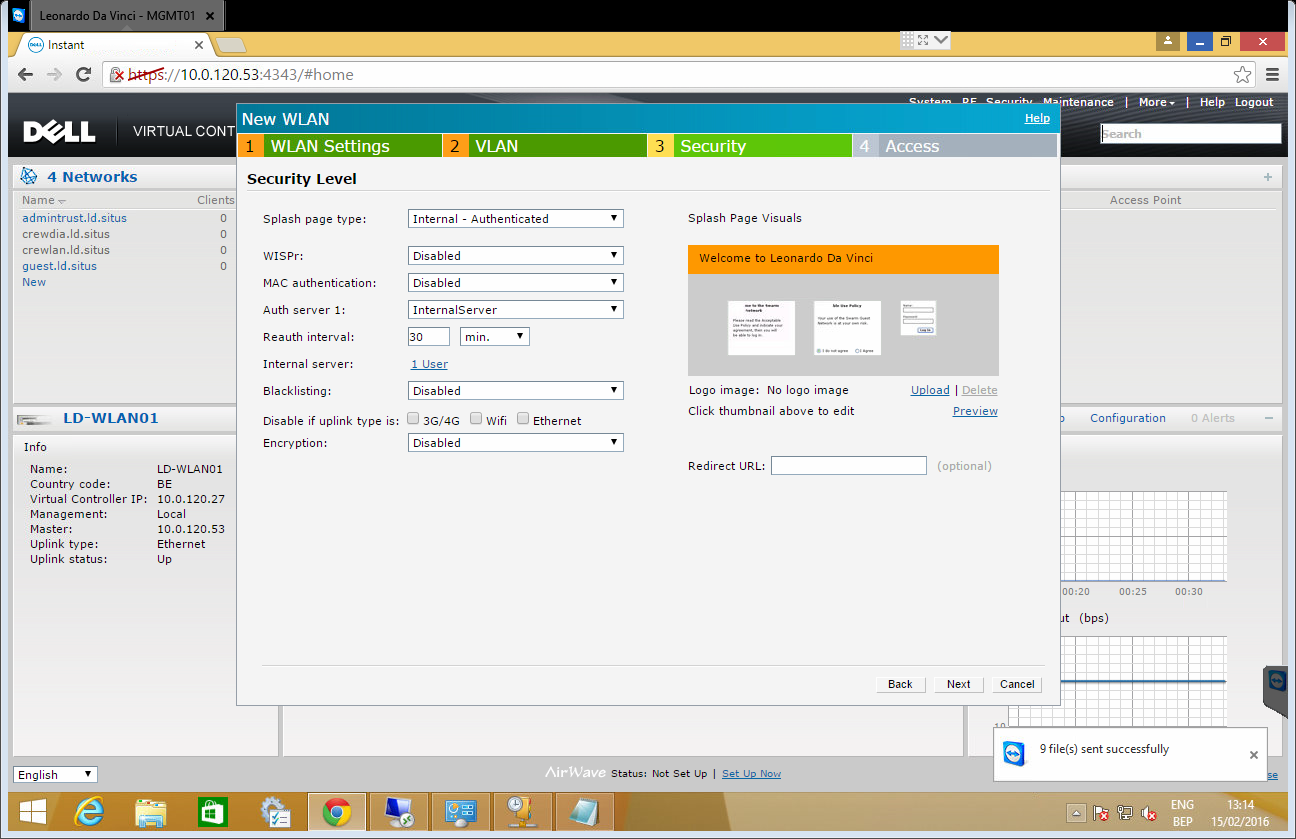
"Next"

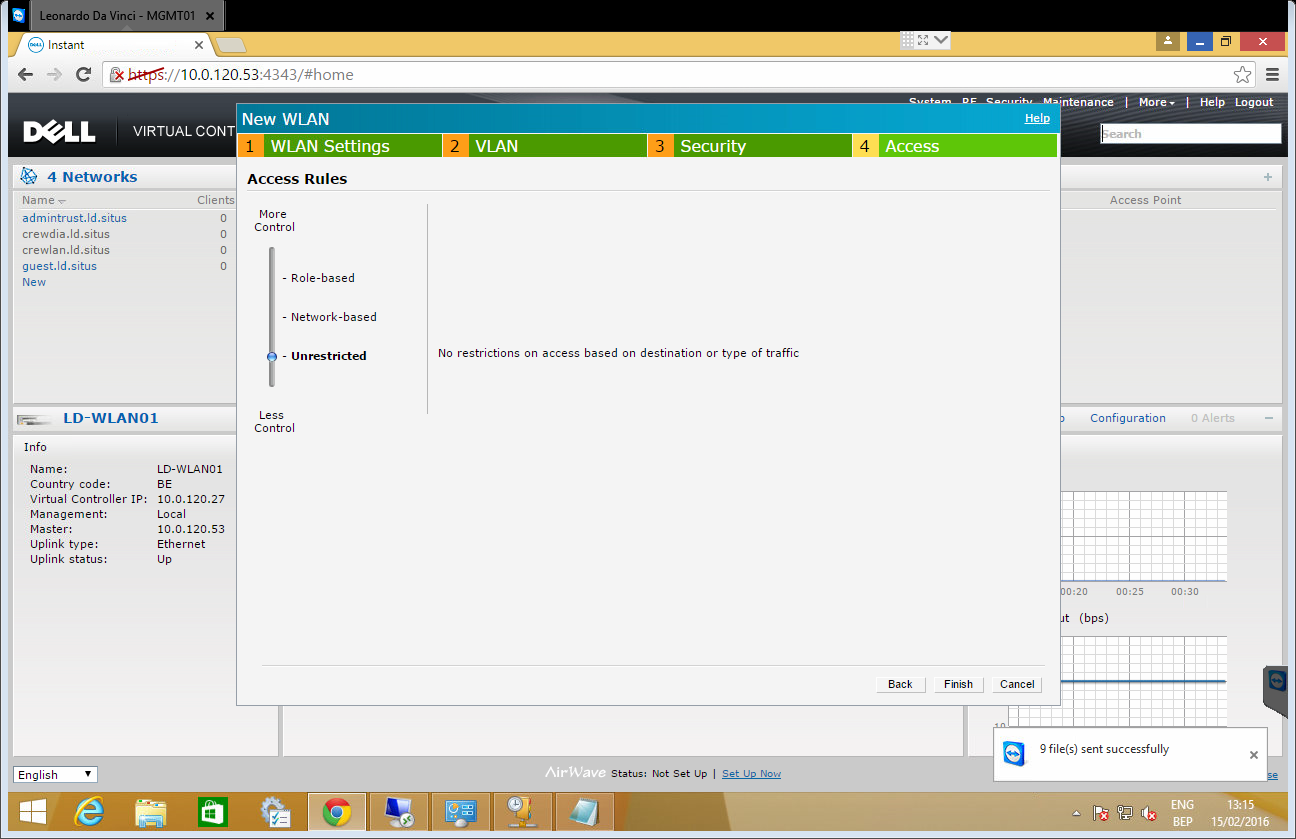
* Client IP assignment: Network assigned
* Client VLAN assignment: Static
* VLAN ID: 906



"Next"

* Splash page type: "Internal – Authenticated"
* Reauth interval: 30min (this can be raised or lowered based on feedback from the captain or chief)
* Internal server: 1 user
  + guest user
    - Username: <vessel prefix>, example: "ld"
    - Password: <vessel prefix>, example: "ld"



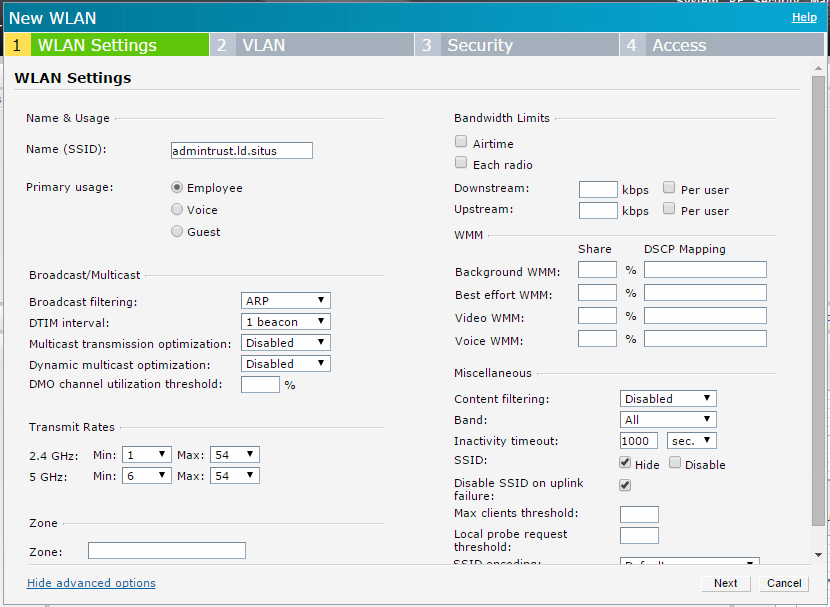


## Sites

### admintrust.\*\*.situs

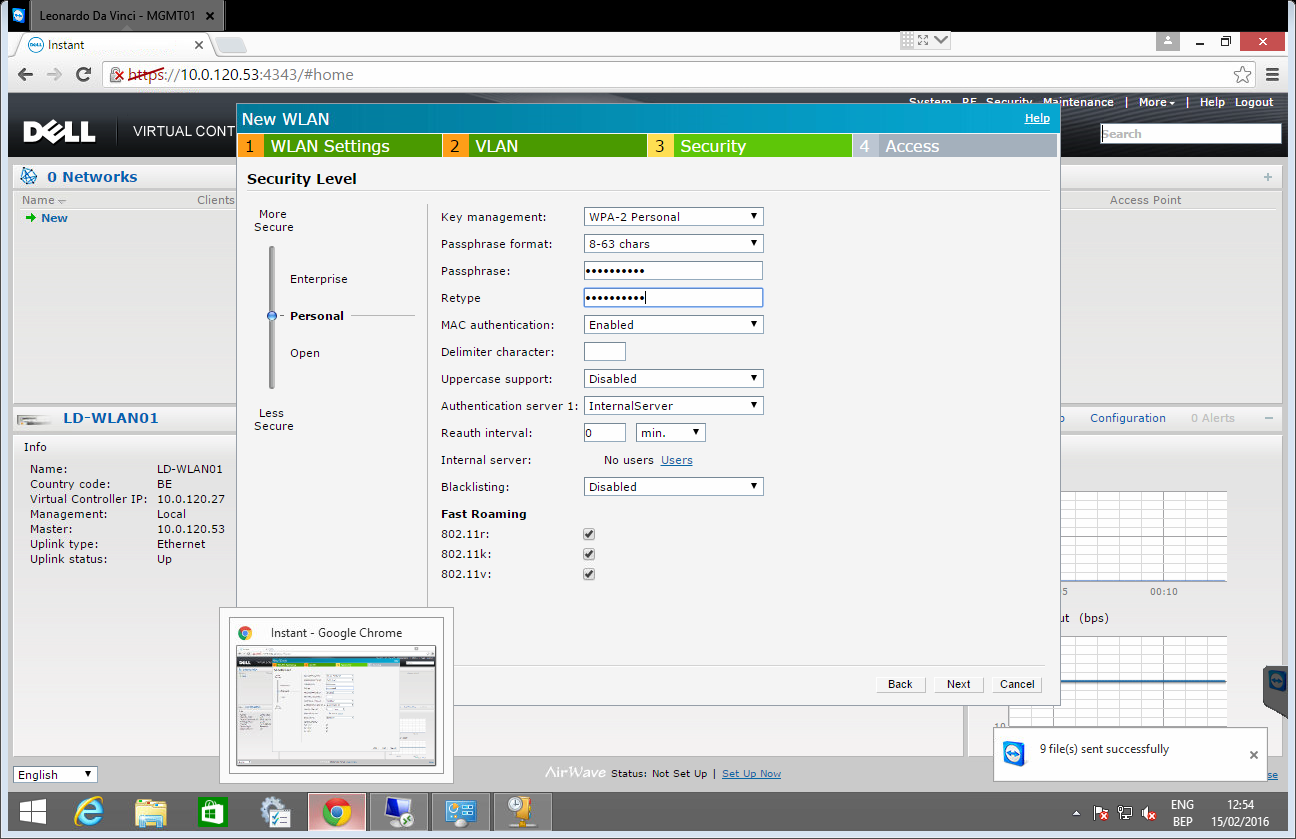
Click on "new" and "Show advanced options"

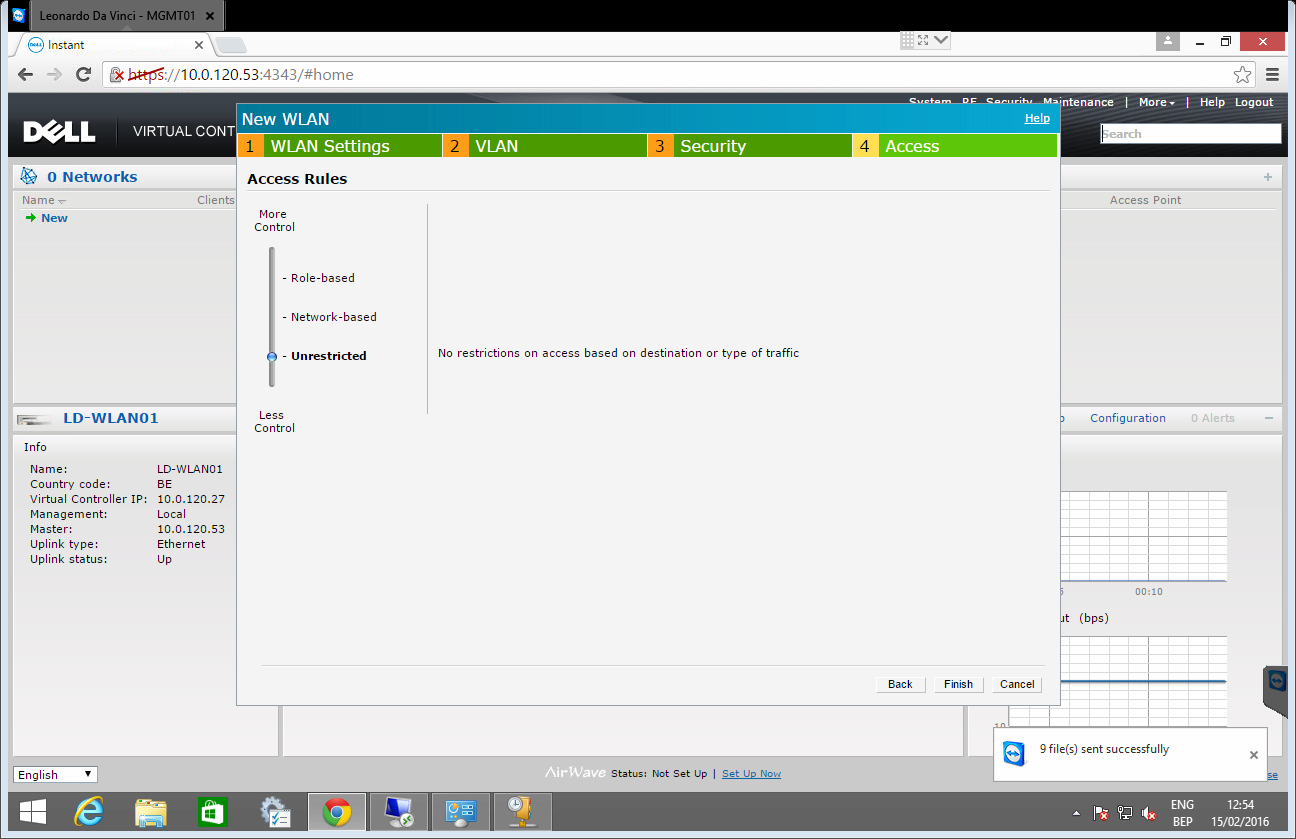
* Name (SSID): admintrust.\*\*.situs
* SSID: Hide



"Next" and change the values below:

* WPA-2 Personal
* Mac authentication: "Enabled"
* Fast roaming: on

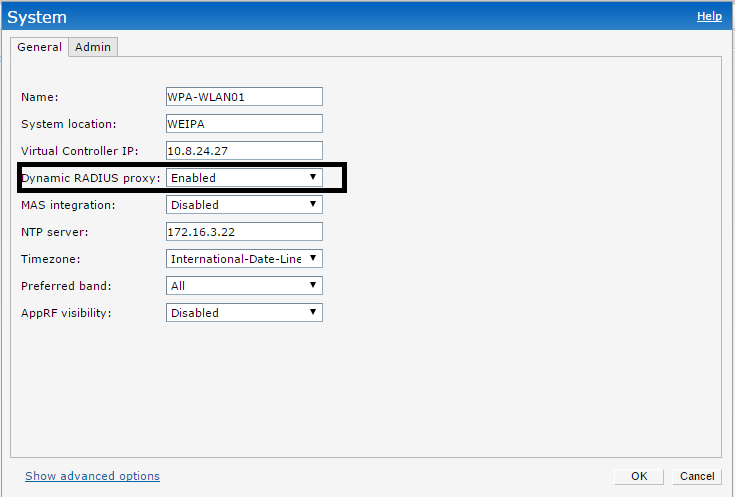




### adminuntrustdata.\*\*.situs

This connection uses RADIUS, make sure SA/SE has added the site as known client on the RADIUS server.

Under System:

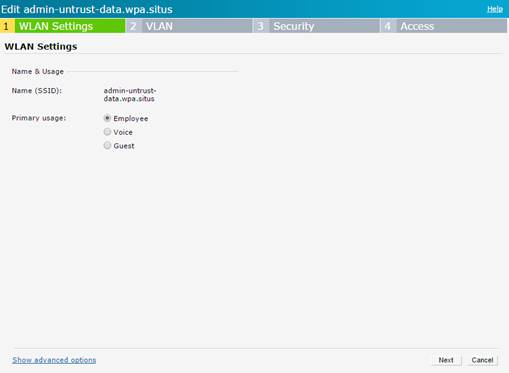


Click on "new" and "Show advanced options"

• Name (SSID): adminuntrustdata.\*\*.situs

• Primary usage: Employee

• SSID: Hide

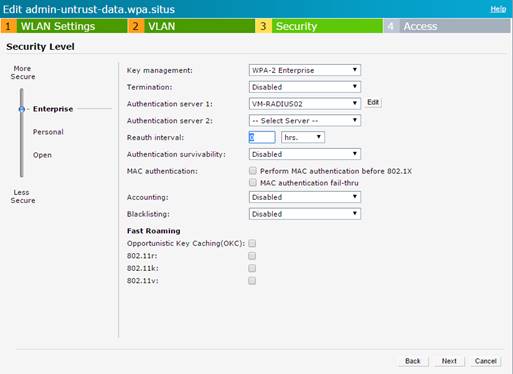


"Next" and change the values below:

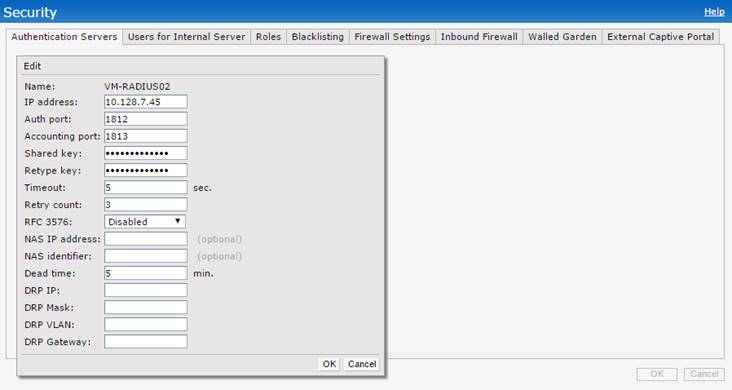
• WPA-2 Enterprise

• Authentication server 1: "VM-RADIUS02" (click edit)

• Fast roaming: off



Under the auth server (edit):

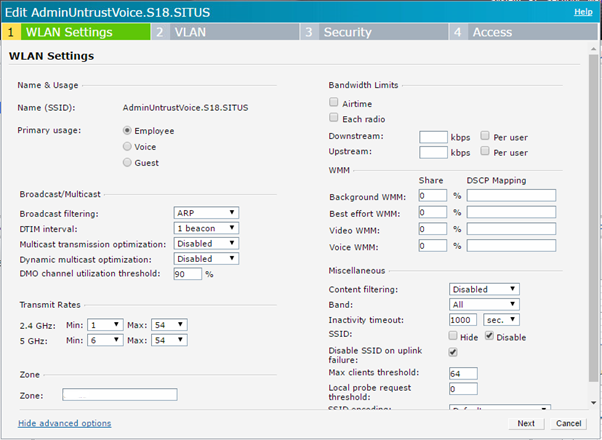


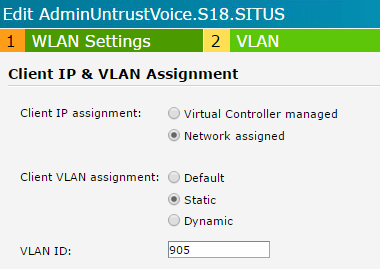
Note: the preshared key can be found in RDM.

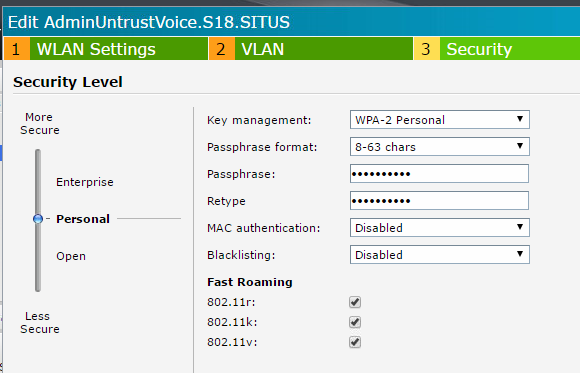
Access rules: unrestricted

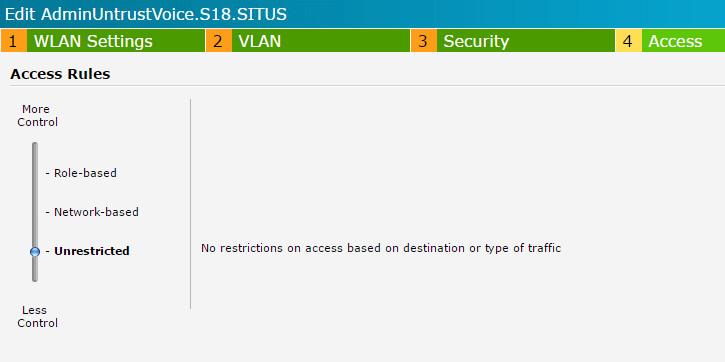


### adminuntrustvoice.\*\*.situs



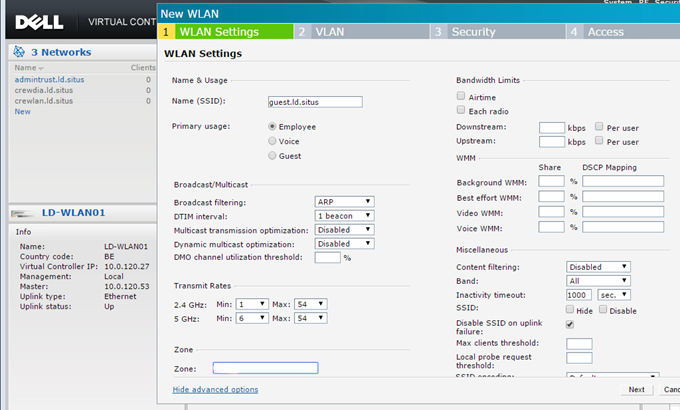






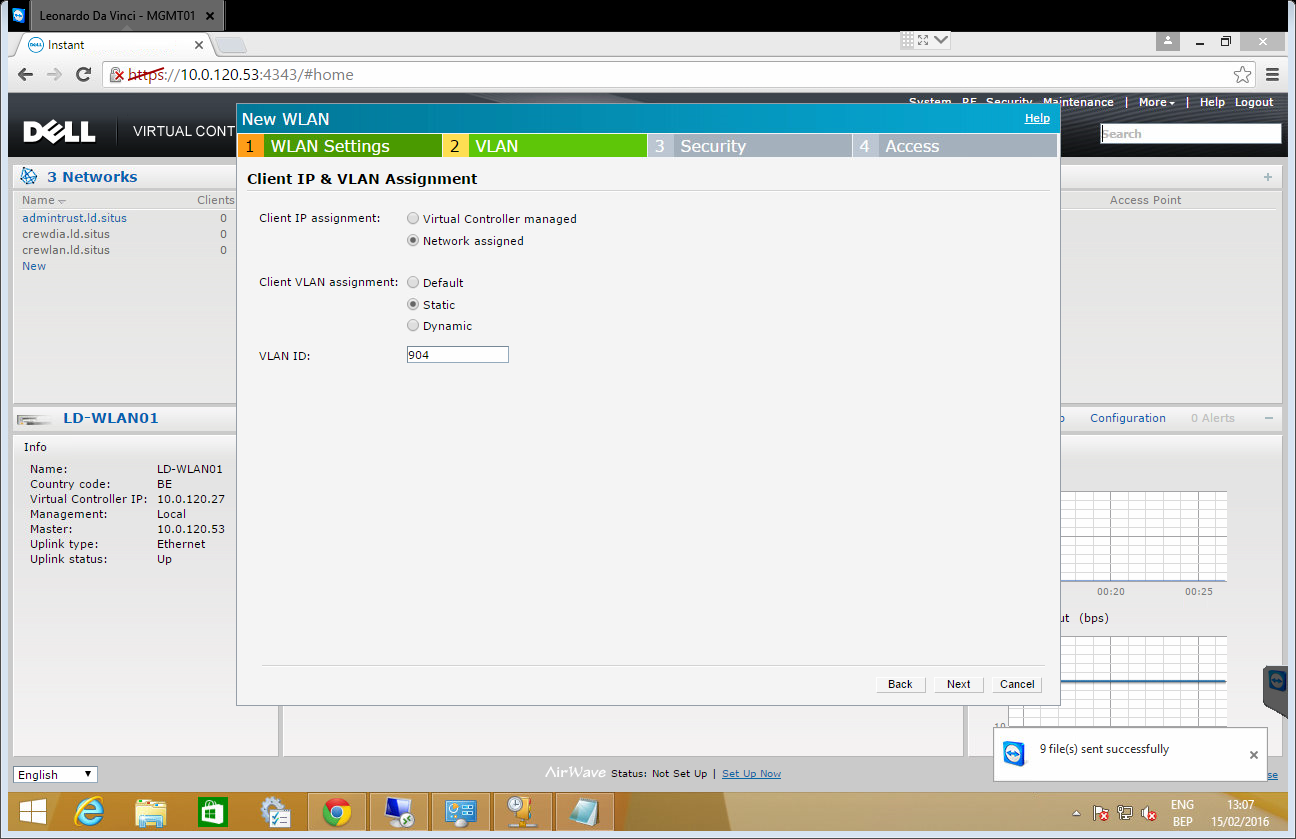
### guest.\*\*.situs

* Name SSID: guest.\*\*.situs



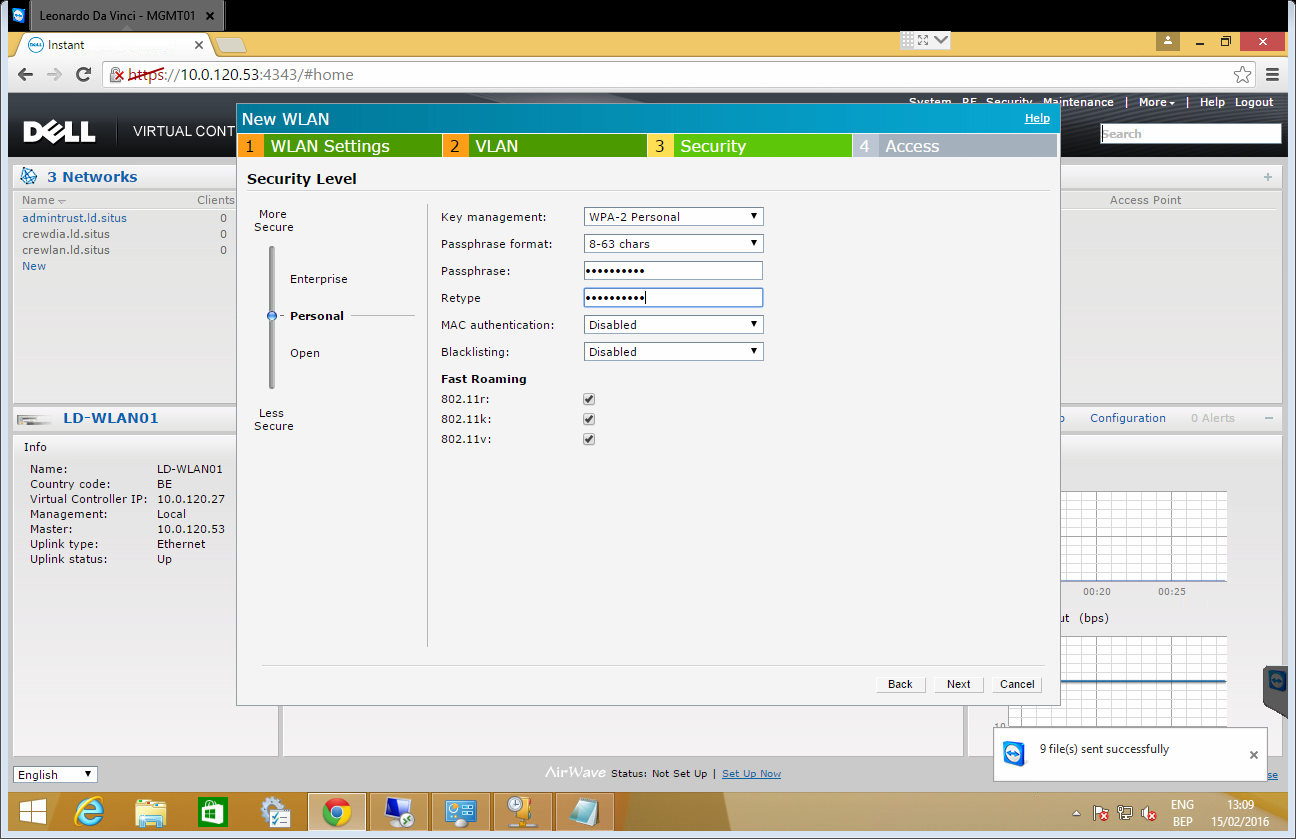
"Next"

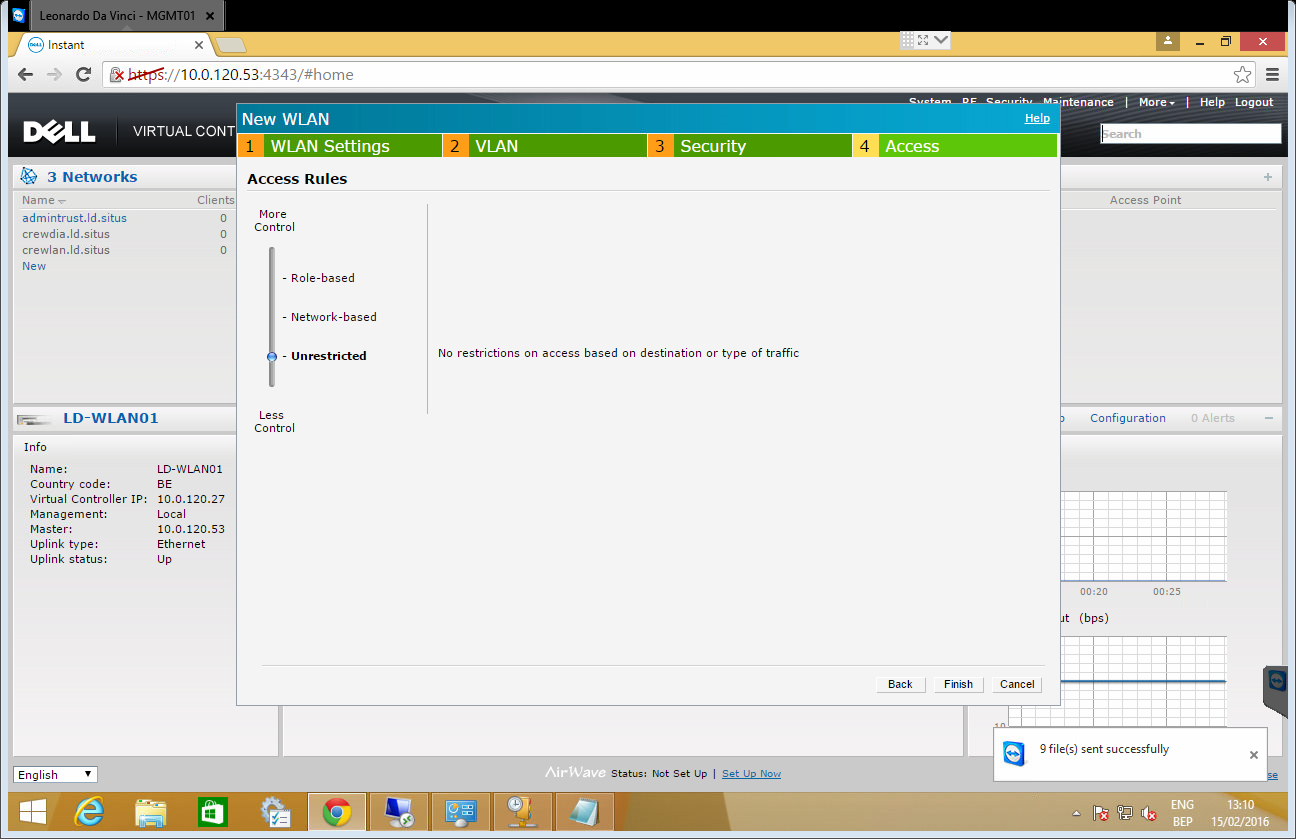
* Client VLAN assignment: Static
* VLAN ID: 904



"Next"

* WPA-2 Personal
* Fast roaming: on



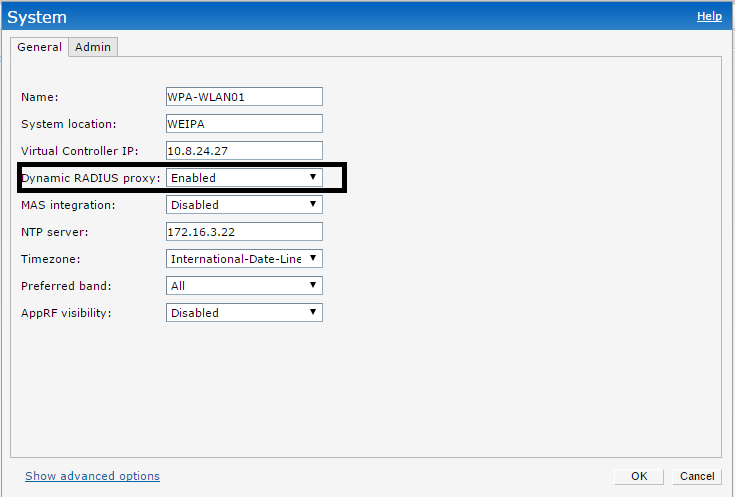


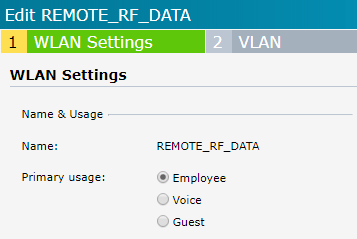
## JDN integrated sites

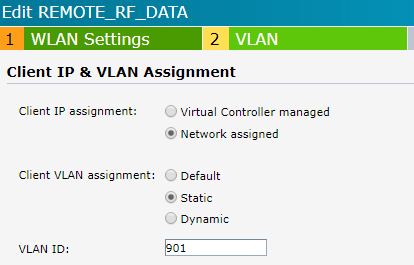
### REMOTE\_RF\_DATA

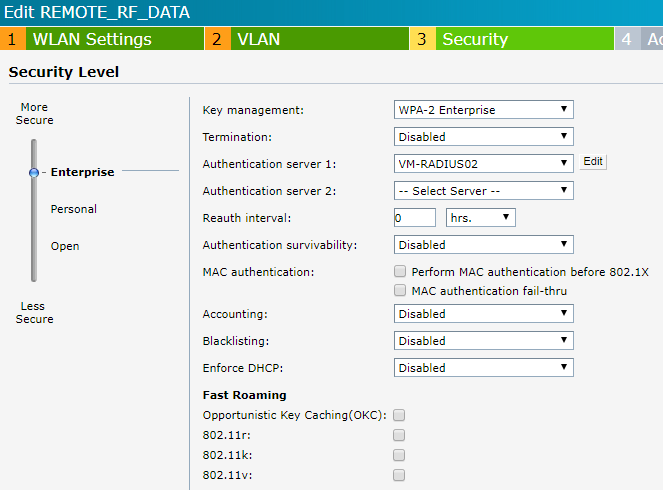
This connection uses RADIUS, make sure SA/SE has added the site as known client on the RADIUS server.

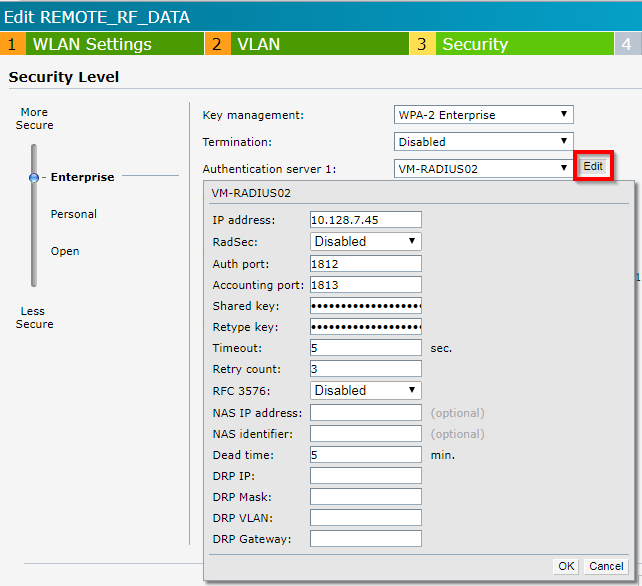
Under System:

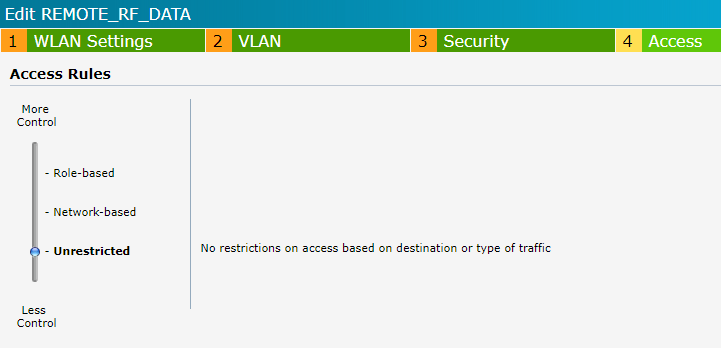




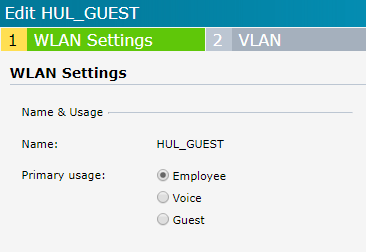


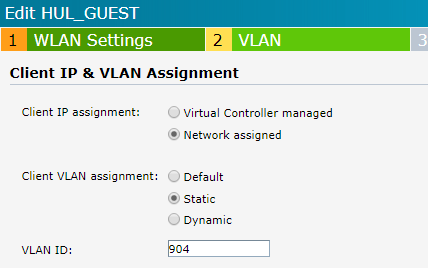


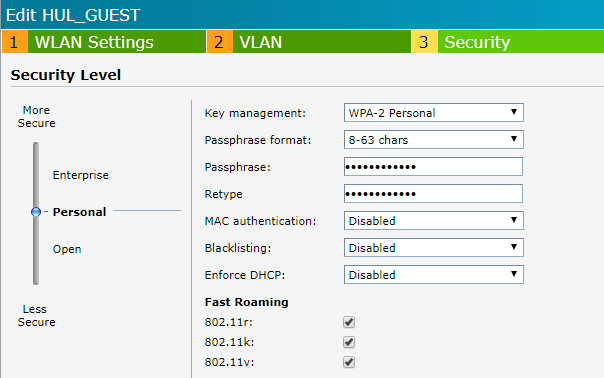


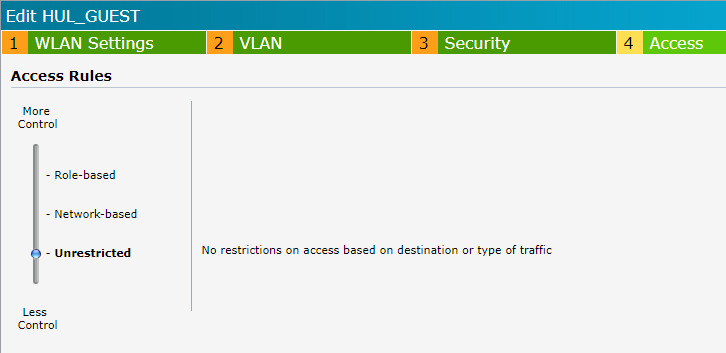


### XXX\_GUEST









# 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.

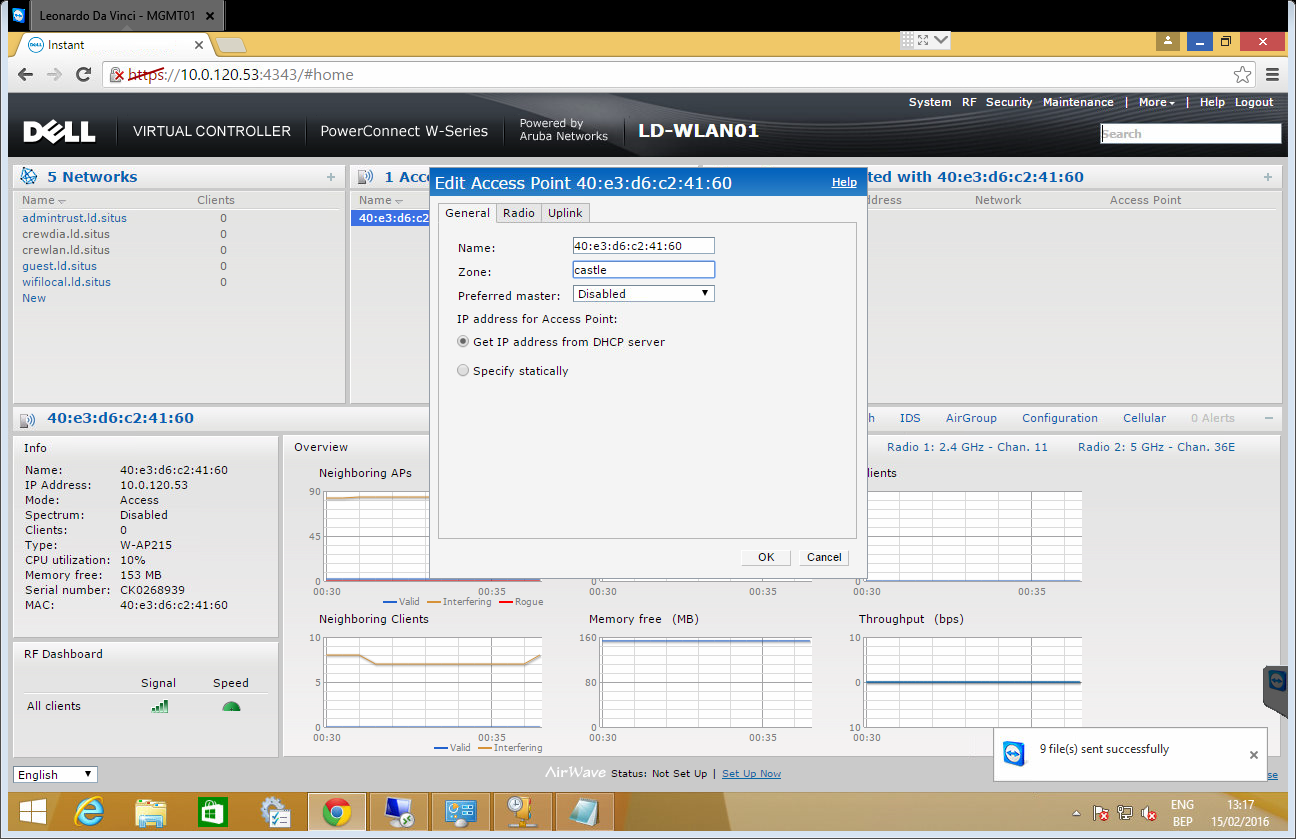
SSID’s without a tag a broadcasted by every AP. (admintrust.\*\*.situs)

### 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.



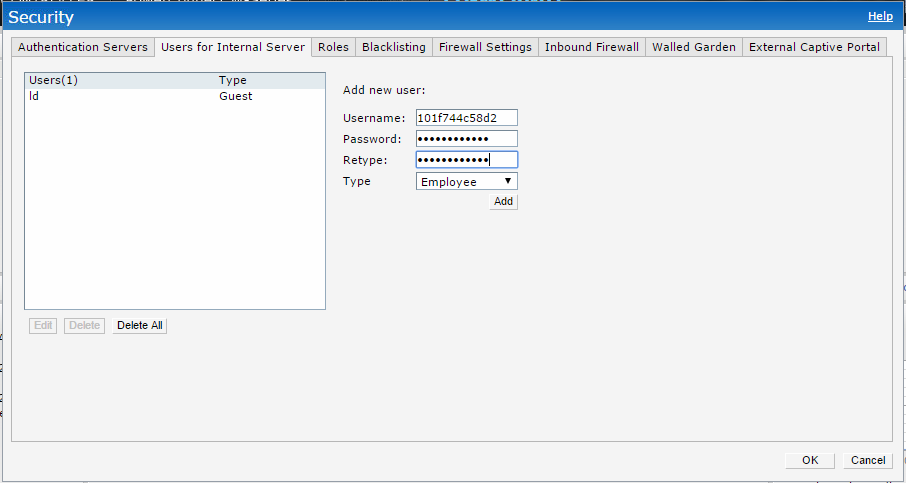
# Whitelisting the MAC address of a barcode scanner

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

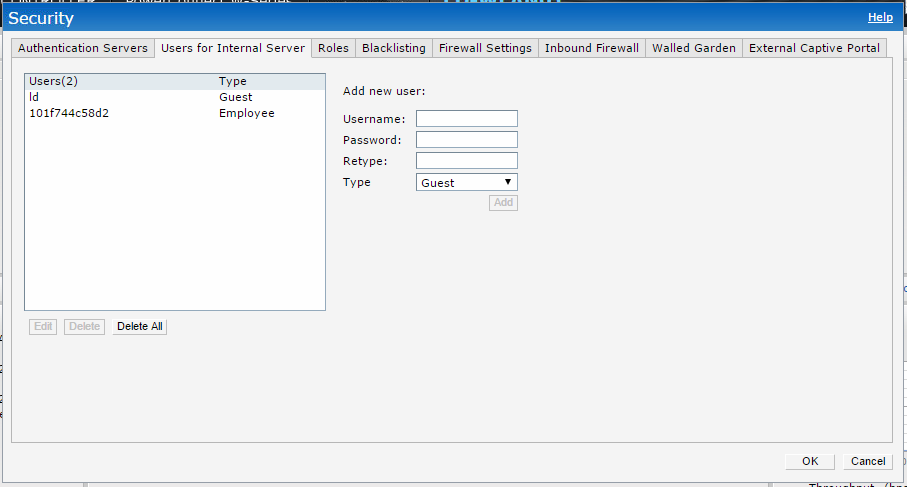
"Add new user:"

* 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.

