

iKnos Corporate

INSTALLATION GUIDE



ARUBA On-prem
Integration Guide

iKnos Corporate by Foot Analytics

Last revision
November 2022

CONTENTS

ARUBA ON-PREM Integration	2
IAP Integration	2
Controller Integration	2
ALE Integration	3

ARUBA ON-PREM Integration

Three different methods are available when connecting Aruba data:

- IAP to Foot Analytics ALE
- Customer Controller to Foot Analytics AKE
- Customer ALE to Foot Analytics ALE

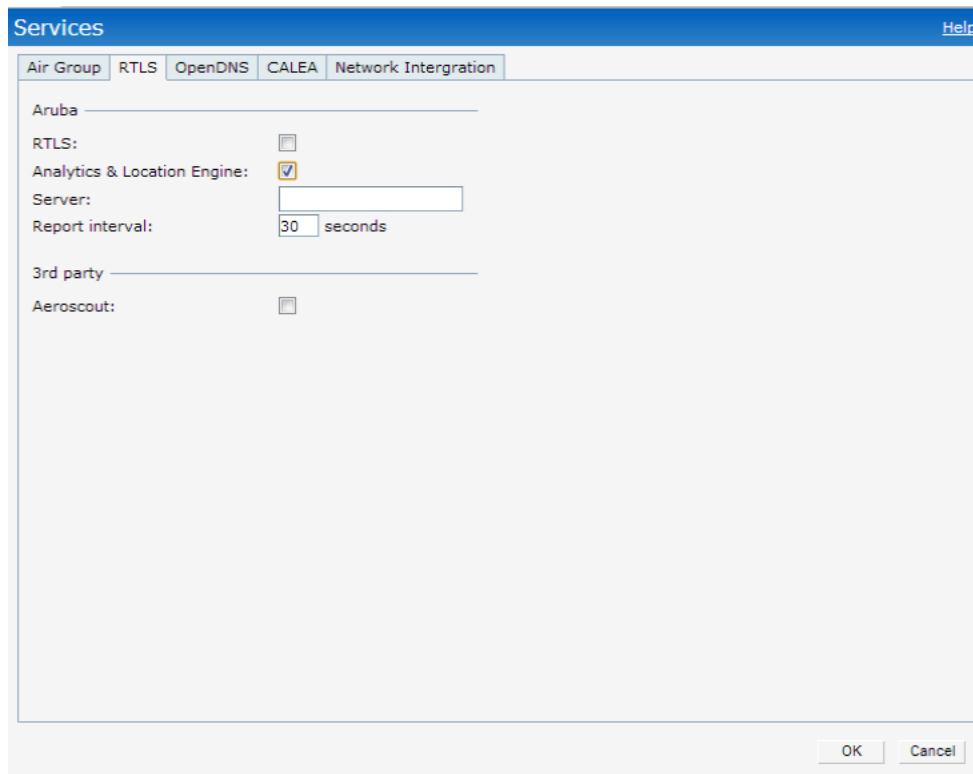
IAP Integration

IAP (Instant Access Points) can be **connected directly** to our ALE in two ways: using the CLI or **Instant UI** (recommended).

Connection data needed by the customer:

- Server: ale.foot.bi
- Port: **8855**

The UI / form might be like the following:



The screenshot shows a configuration window titled "Services" with a "Help" link in the top right corner. The window has several tabs: "Air Group", "RTLS", "OpenDNS", "CALEA", and "Network Intergration". The "Network Intergration" tab is selected. Under the "Aruba" section, there are four items: "RTLS:" with an unchecked checkbox, "Analytics & Location Engine:" with a checked checkbox, "Server:" with a text input field, and "Report interval:" with a numeric input field set to "30" and the unit "seconds". Under the "3rd party" section, there is "Aeroscout:" with an unchecked checkbox. At the bottom right of the window, there are "OK" and "Cancel" buttons.

Controller Integration

IAPs send the data to the **customer controller**, which **forwards** it to Foot Analytics' ALE.

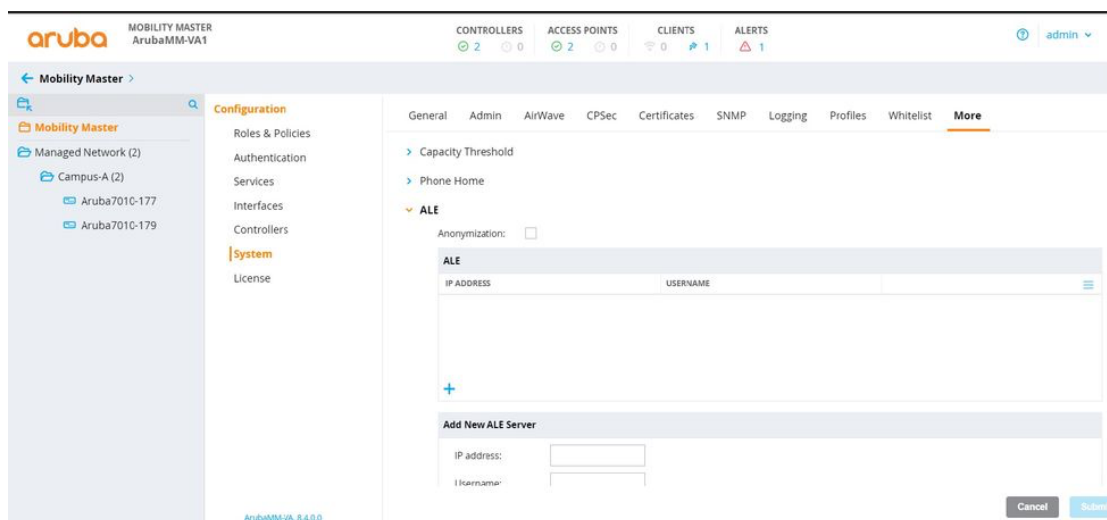
Connection data needed by the customer:

- **User:** To be defined with the customer
- **Password:** To be defined with the customer
- **Server:** ale.foot.bi
- **Port:** [8855](https://ale.foot.bi)

Connection data needed by Foot Analytics:

- Customer controller **IP address**

The UI / form might be like the following:



ALE Integration

A **WebSocket tunnel** is established between two ALEs.

The customer's ALE acts as a WebSocket client, and Foot Analytics' ALE acts as a WebSocket server which receives the customer data.

The customer must configure their ALE server by applying the following configuration:

ALE > Options > Websocket Tunnel

The UI / form it's like the following:

The screenshot shows a web interface for configuring an ALE. On the left is a navigation menu with categories: Monitoring, Configuration, Mode, Source, Options (highlighted in orange), Admin, and Maintenance. The main content area is titled 'General' and contains several dropdown menus: 'NTP Server', 'WebSocket Tunnel', and 'Local End-Points'. Below these are two tables for defining endpoints. The 'Local End-Points' table has columns for 'LOCAL ENDPOINT' and 'PORT #', and is currently empty with a '+' icon for adding a new entry. The 'Remote End-Points' table has columns for 'REMOTE ENDPOINT URL' and 'PORT #', and is also empty with a '+' icon. At the bottom, there are three checkboxes: 'No SSL', 'Trust Invalid SSL Certificate', and 'Enable 2-way Authentication', all of which are currently unchecked.

Then the following configuration must be added:

1. Add a local endpoint with the following parameters:
 - **Host:** localhost
 - **Port:** 7778
2. Add a remote endpoint with the following parameters:
 - **Server:** ale.foot.bi
 - **Port:** 443