IMS Integration Guide

Prepared for:

IMS Customers
5th July 2019

Document Details:
Version 1.8.3.0

FTP SOLUTIONS

Level 10,
182 St Georges Terrace,
Perth, WA, 6000

otsc@ftpsolutions.com.au
(08) 6355 5281
ftpsolutions.com.au

Document name	IMS Integration Guide
Version	1.8.3.0
Version date	5 July 2019
Created by	Steven Brown
Approved by	Acea Quigg

1. Version History

Version should be the current IMS release version with an extra number. I.e. for IMS version 1.8.2, the IMS Integration Guide should have a version 1.8.2.X. Increment X as required.

Date	Version	Author	Description of Change
22/03/2017	1.0	Steven Brown	Created
24/10/2017	1.1	Acea Quigg	Added GIS info
25/10/2017	1.2	Acea Quigg	Added remote access requirement
26/10/2017	1.3	Acea Quigg	Added FTP IPs
12/04/2018	1.4	Acea Quigg	Added distributed IMS info
19/07/2018	1.5	Acea Quigg	Updated for IMS 1.7
10/09/2018	1.6	Acea Quigg	Added WebGL requirement
18/09/2018	1.7	Acea Quigg	Added new IMS components
21/03/2019	1.8	Aaron Low	Updated for IMS 1.8
28/05/2019	1.8.2.1	Aaron Low	Updating SRS, SMTP requirement
20/06/2019	1.8.2.2	Acea Quigg	Bandwidth info, more device support
27/06/2019	1.8.2.3	Acea Quigg	Updating NAM and agent ports
5/07/2019	1.8.3.0	Aaron Low	WMI static port information

Contents

FTP SOLUTIONS

Level 10,
182 St Georges Terrace,
Perth, WA, 6000

otsc@ftpsolutions.com.au
+61 8 6355 5281
ftpsolutions.com.au

Please Note:

The document is meant to be an accurate deployment and requirements guide and should be read and thoroughly understood by anyone looking to deploy IMS, both from a technical and non-technical perspective.

It is important to understand the IMS' requirements and ensure that they are met. The requirements set out in this document are exactly that, requirements. Very few things are nice to haves, rather they are a necessity. In saying that though, FTP is always happy to work with customers and provide alternate solutions where network security or environmental challenges become a concern, especially in the likes of AHS environments.

IMS access for integration and support activities seems to field the most questions and is generally met with the most opposition, and rightly so. We acknowledge that outbound connections from the IMS server back to the FTP office servers may appear to be a nice to have, but, in reality, are a necessity.

These outbound connections allow the deployed IMS server to receive application and security updates, allow IMS server health to be monitored proactively and they also allow FTP support staff to provide customer support when customers pose questions or experience technical difficulties.

If outbound connectivity can't be permitted, then there are many other options, such as a direct VPN connectivity and direct SSH connectivity, as long as this allows for an OSX machine to directly communicate via IP to the target IMS server.

IMS is managed with a set of robust deployment tools that manage IMS versioning, system requirements, software requirements, system optimisation, backup and rollback functionality. Without the ability to use the IMS deployment tools the job of supporting and maintaining IMS becomes a burden of concern for FTP and will fall into a different category of support where the customer will be charged for support by the hour, rather the usual free application support. In the absolute worst case, it is possible to fly a technician to site once a year to update IMS or when as is required, FTP can provide pricing for this option if required.

2. Document Intent

The Intent of this document is to provide clients with a technical overview of the steps and processes associated with the implementation and enablement of the Integrated Management System (IMS) at a customer's site.

FTP SOLUTIONS

Level 10,
182 St Georges Terrace,
Perth, WA, 6000

otsc@ftpsolutions.com.au
+61 8 6355 5281
ftpsolutions.com.au

3. Technical Overview

Refer to Annex A for architecture diagram

The IMS software operates on a virtual machine; the architecture within the IMS is broken down as:

- IMS frontend (approximate)
  - Nginx web server (SSL)
- IMS API (approximate)
  - Brokers connections between the frontend and the backend
  - Caches data
  - Limits requests
  - Provides a data pipeline to request or save data in the backend
- IMS backend (approximate)
  - Trailer and Vehicle device monitoring
  - Backhaul device monitoring
  - Server monitoring
  - Power system (solar/generator) monitoring
  - Availability monitoring
  - ICMP ping streams
  - SNMP streams (hardware dependant)
  - HTTP/HTTPS streams (hardware dependant)
  - SSH streams (hardware dependant)
  - Location sources
    - FMS API and/or database tie-in
    - Intermittent streams to trailer GPS data source (hardware dependant)
- IMS database
  - PostgreSQL
  - Holds all of the IMS data
- IMS message queue
  - Internal IMS message queue
  - Provides a message bus for inter-module communications
- IMS messenger service
  - Sends physical emails, alerts, reports and other messages outbound
- IMS report generator
  - Responsible for creating reports utilising IMSQL
- IMS imagery
  - Generates flyover and terrain imagery
  - Server flyover and terrain imagery

4. Technical Requirements

4.1. User Environment

The user environment will be the standard client desktop or laptop SOE; with the exceptions:

- The latest Google Chrome should be installed to utilise the IMS web GUI
    - Chrome v62 or less must be used if computers have Intel iris 6100s
- For users, whose job it will be to focus on the IMS application, it is recommended that a dedicated graphics processor is installed, a Nvidia GTX 950 or better or AMD equivalent
- For users who will be checking on the IMS for statistics and reporting, a standard laptop with integrated graphics will be sufficient, however, a dedicated GPU is recommended.

4.1.1. IMS User Hardware Configurations

4.1.1.1. User Desktop

- Ubuntu 16.04 desktop/OSX 10.10/Windows 7 or newer
- CPU – 4 x 2GHz+ cores
- RAM – 4GB
- Storage – 80GB HDD
- Google Chrome 64-bit (v58 or above)
- Dedicated 3D graphics accelerator (where applicable)
    - Nvidia GTX 950 or better or AMD equivalent
- Correct graphics drivers to ensure best performance
- WebGL enabled in Chrome and the user's SOE
- Client corporate network connectivity to IMS server; or
- Client corporate VPN access with access to IMS server

4.1.1.2. User Laptop

- As above, with equivalent mobile GPU
    - SSDs are recommended

4.2. Production Environment

4.2.1. Network Access

It is a requirement for the IMS to have routed access to all services, devices and hardware that should be polled/interrogated/accessed/utilised in the gathering and display of fleet and network data. Those requirements include SSH, Telnet, HTTP, HTTPS, MODBUS, SNMP, database access via ODBC and a source of flyover imagery from a system like ArcGIS' RESTful web interface. Access and system requirements are likely to grow over time. A list of ports and protocols is in Annex D

4.2.1. IMS bandwidth requirement

The IMS' bandwidth requirement to the field is heavily dependent on the hardware that is being monitored. It ranges from about 250bps to about 3kbps averaged out over an 8 second polling cycle. As you can imagine, SNMP polling a switch pulls back a fair amount more data than an IMS agent running onboard a Linux radio pushing back data.

IMS bandwidth requirement to the user is somewhat bursty, as it is a dynamic web application. When the user loads the IMS application for the first time the user's chrome browser will load an additional ~2MB of data, which is the IMS application's static data. Every subsequent IMS page load will result in ~6MB of data being first loaded, this includes 30 minutes of live data for the site.

Once the initial data is loaded IMS will stream in new data as it becomes available at a rate of around ~23KB per 8 seconds or roughly 3KB a second per open IMS instance.

4.2.2. IMS VM configuration

The IMS application is usually installed on a single VM. It can be configured and installed in such a way that the IMS components, specifically, the Frontend, API and Backend are installed on separate VMs. You would choose a distributed installation if you have a specific security requirement that requires the IMS users to access a frontend in the corporate network that was then pulling data from an API/Backend that was protected by a site-based firewall. The other reason to choose a distributed installation is if there are a very large number of devices being polled by IMS, ~2500+. It is possible to poll 2500+ devices on a single VM, however the VM specs would become a considerable portion of the physical host's resources and in most cases a physical server would make more sense.

4.2.2.1. Single VM IMS

- OS:
  - Ubuntu LTS Server 18.04 or newer
    - https://www.ubuntu.com/download/server/thank-you?version=18.04&architecture=amd64
    - Ensure to select LVM when partitioning
    - Ensure SSH server module and access is enabled
- CPU:
  - 8 x 2.2GHz if < 50 trucks
  - 12 x 2.6GHz+ if >= 50 trucks
- RAM:
  - 16GB if < 50 trucks
  - 32GB if >= 50 trucks
- Storage:
  - 600GB if < 50 trucks
  - 1TB if >= 50 trucks

**Numbers are not exact, testing and adjusting is required. 'Trucks' is referring to dump trucks, not devices with an IP.*

4.2.2.2. Distributed IMS

- Front-end VM
  - 4 CPU cores
  - 8 GB RAM
  - 50GB storage
- API + database VM
  - 8 CPU cores
  - 22 GB RAM
  - 700GB storage
- Backend + message queue VM
  - 8 CPU cores
  - 10 GB RAM
  - 50GB storage

*Numbers are not exact, testing and adjusting is required

5. IMS Deployment

Integration of assets and devices into the IMS is undertaken by FTP or its agent. The integration team will use the client supplied asset register containing IP address, equipment numbers/types and fixed infrastructure locations, an example of the asset register is at Annex E. The more time spent getting the asset register correct and updated, the quicker IMS will be available and in production.

5.1. Project Kick-off

Once FTP Solutions has received a PO, implementation will begin, and the pre-deployment stage commences.

5.2. Pre-deployment - Data Collection

During the Pre-deployment phase, the steps involved in the Active IMS Deployment stage are outlined, and the information required from the client is sourced and discussed. This is to ensure that all parties are clear on what is involved in deploying IMS. The Pre-deployment phase will focus on:

- Identify the Deployment/Integration Team
  - Project manager
  - Project contacts
    - Infrastructure
    - GIS personnel
    - Fleet management personnel
    - Network team
- Complete and return the Asset Register information, IAW Annex E
  - Fleet management system

        - API/DB access details
        - Transform must be supplied if locations are in local grid. If in a standard SRS, provide the EPSG code.
    - Terrain / high precision management system
        - API/DB access details
        - Transform must be supplied if locations are in local grid. If in a standard SRS, provide the EPSG code.
    - On truck / excavator / drill wireless radio/s
        - Access details
        - IPs
    - Pont to point microwave radio/s
        - Access details
        - IPs
    - Point to multi-point microwave radio/s
        - Access details
        - IPs
- Provide network diagrams
- Provide access to NMS software to speed up IMS deployment
- Build the IMS VM
    - Create 'ftpsolutions' user account
        - Must have sudo rights
- Create service accounts for device polling
    - IAW Annex D
- Create LDAP IMS RO, RW and Manager groups
    - Provide LDAP server details
- Configure SMTP relay for sending IMS notifications and reports
    - Provide SMTP relay details
- Put in change management for any required firewall rules
    - IAW Annex D
- Provide high resolutions site flyover imagery
    - ArcGIS or ERDAS or compatible WMS/WMTS/TMS URL
    - Static file can be supplied
        - Must be georeferenced
        - Transform must be supplied if in local grid. If in a standard SRS, provide the EPSG code.
- Provide 3D xyz terrain file for site
    - Vulcan DXF file, or
    - GeoTIFF, or
    - Esri Shape file, or
    - ASCII x,y,z file

5.3. Pre-deployment - IMS VM Access Requirements

FTP requires access to the IMS VM in order to deploy the IMS software. The easiest way to do that is to provide FTP with a VPN connection to the client's site. Direct SSH or HTTP access is acceptable from the Internet to the IMS VM.

RDP and Citrix are not acceptable forms of network access! The FTP deployment server needs to be able to communicate using TCP/IP directly with the IMS VM that is being integrated.

In the majority of cases, IMS will require outbound access to FTP's servers for licensing and updates:

- 49.255.243.205 (HTTP) for licensing/heartbeat
- 49.255.243.205 (HTTPS) for updates
- 49.255.243.204 (SSH) for support (optional)

5.4. Deployment

Active IMS deployment usually takes around two weeks. During this time FTP will use the information gathered during the pre-deployment phase to populate the IMS with the site's network information. FTP will work with the site to ensure that all devices are being polled and IMS is operating as anticipated. If the site has any technology that IMS does not support new polling engines will be written, providing the technology is in scope.

5.5. Post-deployment

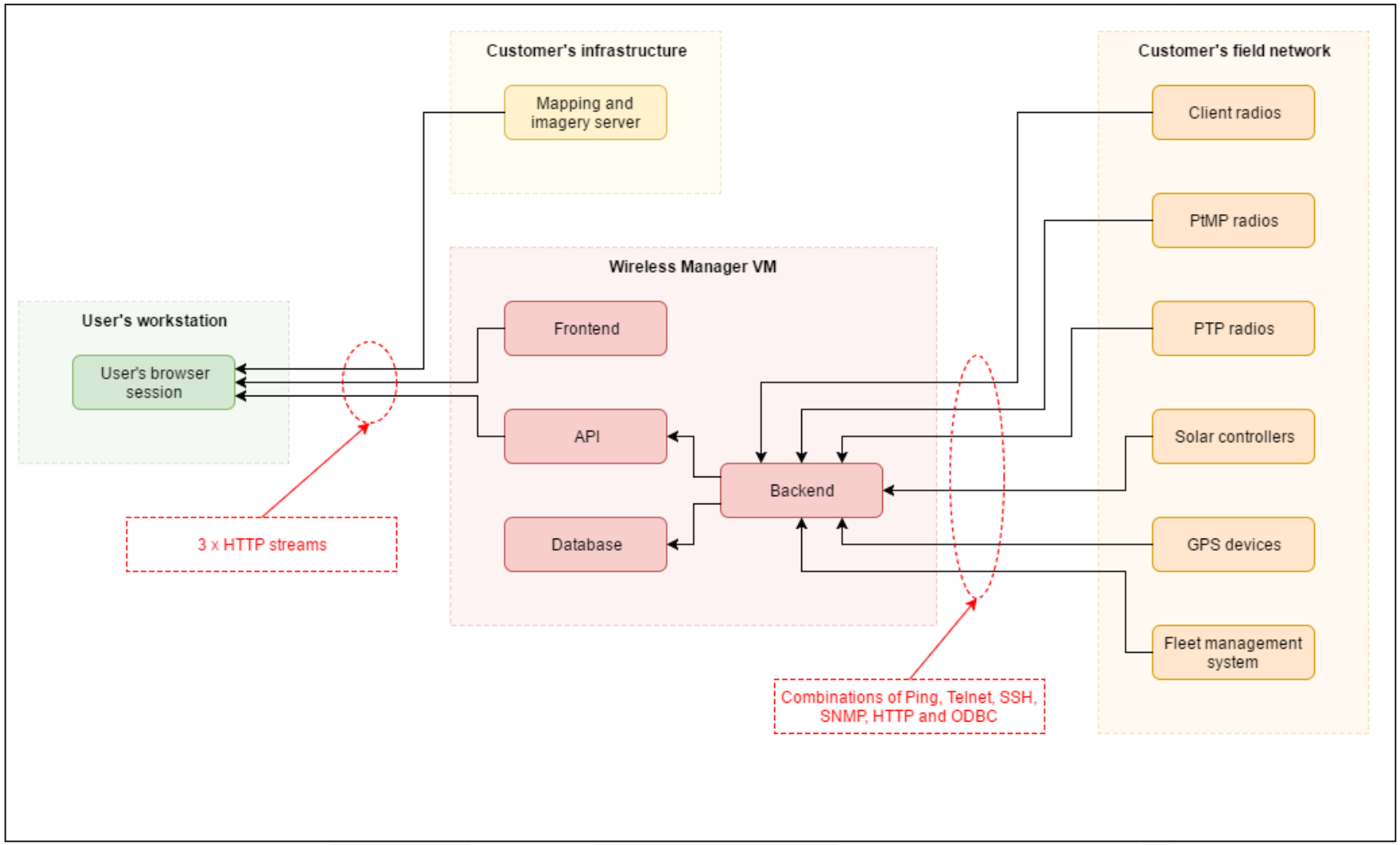
5.5.1. Training

FTP will provide training to the client's relevant personnel on the use of the IMS platform. This training has been developed in a "*train-the-trainer*" format, so as to enable the internal personnel to pass on the relevant training to other potential users. Training time required is typically 6-8 hours and is conducted at either the client's site or FTP's office.

5.5.2. Project Completion / Integration Sign-Off

Once the software has been integrated and accepted by the client, invoicing will follow. Training will be conducted outside of integration on a separate PO.

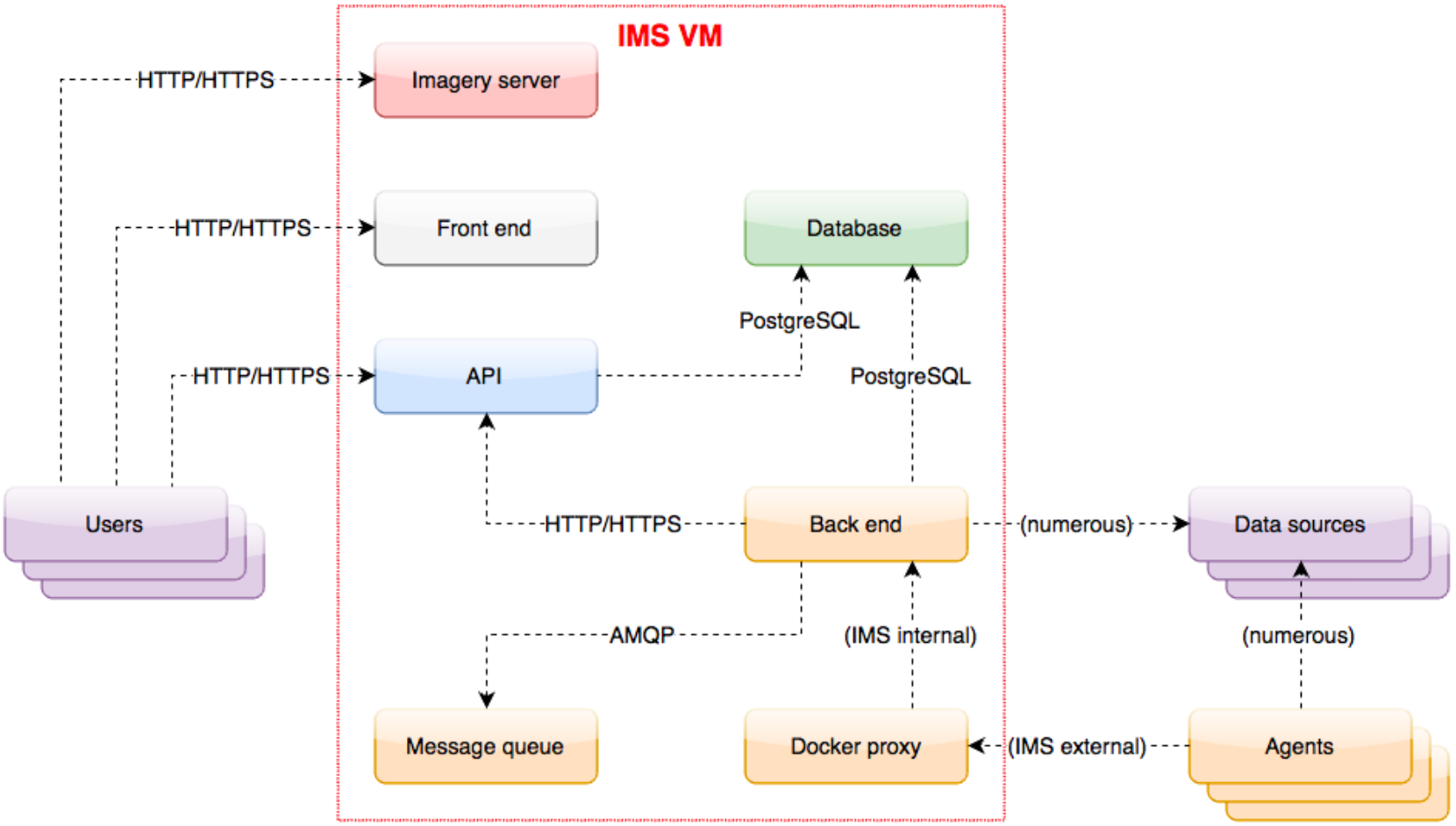
6. Annexure A – IMS Application Overview



Level 10,
182 St Georges Terrace,
Perth, WA, 6000

otsc@ftpsolutions.com.au
+61 8 6355 5281
ftpsolutions.com.au

7. Annexure B – IMS– Single VM Traffic Flows

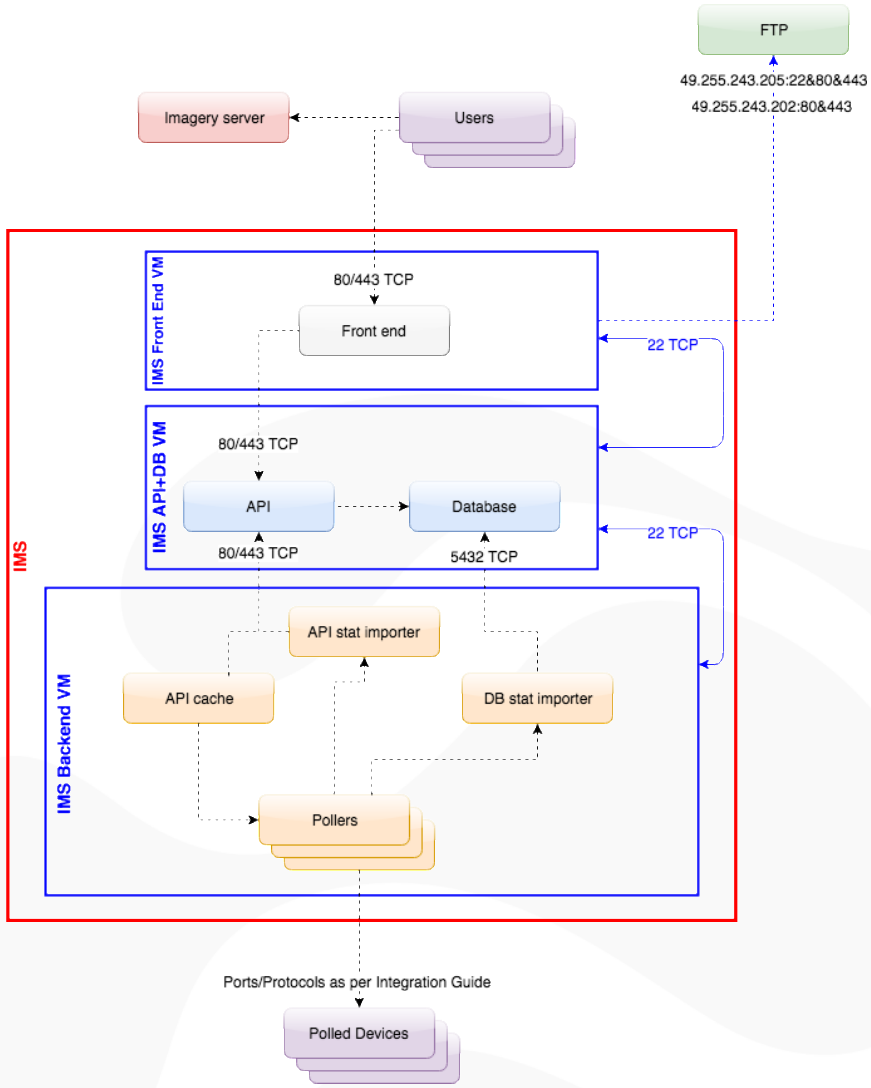


Note: *Any part within the red square is internal to the IMS application. MS SQL for example, is not compatible or needed.*

Level 10,
182 St Georges Terrace,
Perth, WA, 6000

otsc@ftpsolutions.com.au
+61 8 6355 5281
ftpsolutions.com.au

8. Annexure C – IMS Distributed Installation – Traffic Initiation - Ports



Note: *Any part within the red square is internal to the IMS application. MS SQL for example, is not compatible or needed.*

Level 10,
182 St Georges Terrace,
Perth, WA, 6000

otsc@ftpsolutions.com.au
+61 8 6355 5281
ftpsolutions.com.au

9. Annexure D – IMS Ports and Protocols

Network flows (on the corporate side)

Service	Protocol	Source		Destination	
		Host	Port	Host(s)	Port
IMS Frontend	TCP (HTTP/HTTPS)	User workstation	*	IMS VM	80/443
IMS Imagery server	TCP (HTTP/HTTPS)		*	IMS VM	80/443
IMS API	TCP (HTTP/HTTPS)		*	IMS VM	80/443

Network flows (on the operational side when server side polling is used exclusively)

Service	Protocol	Source		Destination	
		Host	Port	Host(s)	Port
Polling engines (all)	TCP (SSH) TCP (Telnet TCP (HTTP) UDP (SNMP) TCP (HTTPS) TCP (MODBUS) TCP (ODBC) UDP (MODBUS)	IMS VM	*	varied	22 23 80 161 443 502 1433 4800/4900

Note: *Not all polling engines are needed for each site, these ports are provided for guidance only*

Note: *There is no requirement for HTTP, it is shown as a possible example. HTTPS is preferred, customer to provide SSL certificate for IMS.*

IMS Ports and Protocols (continued)

The IMS uses a number of different ports and protocols for different purposes- the most diverse of which are those that make up all the polling engines. Here is a breakdown:

- **Front end**
  - listens on
    - TCP port 443 (HTTPS)
- **API**
  - listens on
    - TCP port 443 (HTTPS)
- **Database**
  - listens on
    - TCP port 5432 (PostgreSQL backend protocol)
- **Message queue**
  - listens on
    - TCP port 5672 (AMQP)
    - TCP port 15672 (HTTP on custom port for administration)
- **Imagery server**
  - Listens on TCP port 6080 (HTTP on custom port)
- **Back end**
  - Interacts with devices using IMCP (ping) and, or
    - 3DP e200 Hornet using SSH (TCP 22)
    - 3DP e200 Hornet using IMS agent protocol (UDP 13339 in and 13338 out)
    - AVI 9/8/3 series Modems/Routers using SSH (TCP 22)
    - AVI CCMS using custom protocol (UDP 3337)
    - Aviat radio using SNMP (UDP 161)
    - Axis Q-series camera using HTTP (TCP 80)
    - Cambium PMP4xx device using HTTP (TCP 80)
    - Cambium PTP6xx microwave radio using HTTP (TCP 80)
    - Cambium PTP8xx microwave radio using SNMP (UDP 161)
    - Cambium ePMP device using SSH (TCP 22)
    - Cisco Wireless LAN Controller using SSH (TCP 22)
    - Cisco switch using SNMP (UDP 161)
    - Cisco wireless access point (nothing, data comes from WLC)
    - Cisco workgroup bridge using SNMP (UDP 161)
    - ESXi host using SNMP (UDP 161)
    - Exalt microwave radio using SNMP (UDP 161)
    - Extreme AP71xx access point using SSH (TCP 22)
    - Extreme AP75xx access point using SSH (TCP 22)
    - Extreme RFS Controller using SSH (TCP 22)
    - Fluidmesh 4200 using SNMP (UDP port 161) and SSH (TCP 22)
    - FTP TracBox (server-side) using HTTP (TCP 80)
    - Generic SNMP / TFTP polling engine using SNMP (UDP 161 and 69)
    - Huawei AR-series router using SNMP (UDP 161)
    - Hyper-V Host using SNMP (UDP 161)
    - Komatsu FrontRunner using custom protocol (UDP 3338)
    - Linux System using SSH (TCP 22)

- MTGA Thumb GPS (server-side) using HTTP (TCP 80)
- Mikrotik RB-series access point using SNMP (UDP 161)
- MineStar Fleet orCommand FMS server using HTTP (TCP 8080)
- MineStar Terrain FMS server using ODBC (TCP 1433)
- MineStar TOPE NAM receiver (UDP in 13337)
- Motorola IAP access point using SNMP (UDP 161)
- Modular Dispatch 5/6 using ODBC (TCP 1433)
- Modular ProVision 3.x using ODBC (TCP 1433)
- Moxa/Trimble - TCP 4001 using a custom protocol (TCP 4001)
- Moxa N-port version information using telnet (TCP 23)
- OpenWrt wireless router using SSH (TCP 22), or
- OpenWrt router using IMS agent protocol (UDP 13339 in and 13338 out)
- Other (nothing, ping-only polling)
- RAD Airmux device using Telnet (TCP 22) and HTTP (TCP 80)
- Radwin 2xxx device using SNMP (UDP 161)
- Redline 3xxx device using SNMP (UDP 161)
- Redline 5xxx device using SNMP (UDP 161)
- SAF microwave radio using SNMP (UDP 161)
- Siklu Etherhaul using HTTP (TCP 80)
- Sony IPELA camera using HTTP (TCP 80)
- Strix radios using SNMP (UDP 161)
- TriStar MPPT using HTTP (TCP 80)
- Ubiquiti AirOS device using SSH (TCP 22)
- Ubiquiti device with FTP Firmware using HTTP (TCP 80)
- Wenco FMS server using ODBC (TCP 1433)
- Windows Servers using WMI (TCP 135 then a random negotiated port)
    - For static WMI port config see here
- Windows Systems using WMI (TCP 135 then a random negotiated port)
    - For static WMI port config see here

10. Annexure E – Example Asset Register

Asset Name	IP Device Type	IP Device Name	IP Device IP	SNMP String	HTTP U/P	SSH U/P
TA4298	Cisco 1572	TA4298-AP	10.10.42.1	public	N/A	cisco/pass
	Cambium 450	TA4298-SM	10.10.42.2	public	root/pass	root/pass
	Tristar MPPT	TA4298-MPPT	10.10.42.3	N/A	N/A	N/A
	Cisco IE3000	TA4298-SW	10.10.42.4	public	N/A	cisco/pass
DT2336	Cisco 3702	DT2336-WGB	10.10.52.1	public	N/A	cisco/pass
	G407	DT2336-G407	10.10.52.2	N/A	N/A	N/A
	DSS	DT2336-DSS	10.10.52.3	N/A	admin/pass	Admin/pass
	Cisco IE2000	DT2336-SW	10.10.52.4	public	N/A	cisco/pass

The idea is to list out all the devices that need to be monitored by IMS. FTP needs to be able to associate IP devices (e.g. radios) with assets (e.g. trucks) and know how to poll them (e.g. usernames/passwords/strings etc.). This also includes things like wireless controllers, databases, servers (WMI) etc.